सूचना एवं साइबर सुरक्षा नीति

दस्तावेज़ कोड: - हडको/आईटी-नीतियाँ/2024/03

दस्तावेज़ वर्गीकरण: आंतरिक

(संस्करण 1.1)

हाउसिंग एण्ड अर्बन डेवलपमेंट कॉर्पोरेशन लिमिटेड

कोर-7ए, हडको भवन, इंडिया हैबीटेट सेंटर, लोधी रोड,

नई दिल्ली-110003

वेबसाइट : www.hudco.org.in CIN: L74899DL1970GOI005276

संस्करण इतिहास

क्रम सं.	संस्करण सं.	प्रस्तुतकर्ता	जाँचकर्ता	समर्थनकर्ता	तिथि
1.	1.0	डेलॉइट कॉर्पोरेट फाइनेंस सर्विसेज इंडिया	कार्यकारी निदेशक (आईटी)	हडको बोर्ड	08.01.2019
2.	1.1	एकेएस आईटी सर्विसेज प्राइवेट लिमिटेड	कार्यकारी निदेशक (आईटी)	हडको बोर्ड	16.12.2024

विषयसूची

1. परिचय

सूचना एवं साइबर सुरक्षा नीति, सूचना प्रणालियों और सूचना के किसी भी अन्य उपलब्ध स्वरूप को साइबर हमलों सहित विभिन्न प्रकार के खतरों से बचाने के लिए संरचना और दिशा प्रदान करती है ताकि सूचना परिसंपत्तियों की सुरक्षा, क्षति को न्यूनतम करने और व्यावसायिक निरंतरता सुनिश्चित की जा सके। यह नीति कई खंडों में विभाजित है, जहाँ प्रत्येक खंड हडको की सूचना परिसंपत्तियों और सूचना प्रणालियों की सुरक्षा के लिए महत्वपूर्ण एक ही क्षेत्र को कवर करता है।

2. सूचना और साइबर सुरक्षा उद्देश्य

हडको में सूचना सुरक्षा निम्नलिखित उद्देश्यों से प्रेरित है:

- गोपनीयता बनाए रखते हुए अनधिकृत नियंत्रण से सूचना की सुरक्षा।
- सूचना की अखंडता सुनिश्चित करना। अखंडता का संबंध सूचना की सटीकता और पूर्णता के साथ-साथ व्यावसायिक मूल्यों और अपेक्षाओं के अनुरूप इसकी वैधता से है।
- अधिकृत और अपेक्षित व्यक्तियों के लिए सूचना की उपलब्धता सुनिश्चित करना। उपलब्धता का संबंध वर्तमान और भविष्य में व्यावसायिक प्रक्रिया द्वारा आवश्यकता पड़ने पर सूचना की उपलब्धता से है। यह आवश्यक संसाधनों और संबंधित क्षमताओं की सुरक्षा से भी संबंधित है।
- डेटा, लेनदेन, संचार और दस्तावेज़ों (इलेक्ट्रॉनिक या भौतिक) की प्रामाणिकता सुनिश्चित करना।
- वैधानिक आवश्यकताओं को पूरा करना।
- व्यावसायिक निरंतरता योजनाओं का निर्माण, रखरखाव और परीक्षण।
- सभी कर्मचारियों को सूचना सुरक्षा जागरूकता प्रशिक्षण प्रदान करना।
- सुरक्षा उल्लंघनों की रिपोर्टिंग और जाँच।

हडको में साइबर सुरक्षा निम्नलिखित नियंत्रण उद्देश्यों द्वारा संचालित होती है:

- हडको के बुनियादी ढांचे को साइबर खतरों और जोखिमों से बचाने के लिए साइबर घटना का पता लगाने और उससे निपटने हेतु प्रणाली की स्थापना।
- कमजोरियों से जुड़े जोखिम और उन्हें कम करने की लागत के आधार पर कमजोरियों को खत्म करने या कम करने के लिए भेद्यता प्रबंधन प्रक्रिया को औपचारिक रूप देना।

- सभी शेयरधारकों को साइबर संकट प्रबंधन योजना की जानकारी देना।
- वर्तमान सूचना सुरक्षा आवश्यकताओं और बदलते खतरों, आवश्यकताओं और प्रौद्योगिकियों के आधार पर भविष्य की सुरक्षा आवश्यकताओं की मांगों को पूरा करने के लिए सुरक्षा नियंत्रणों की एक सूची प्रदान करना।
- हडको आईटी प्रणालियों के लिए एक व्यापक जोखिम मूल्यांकन प्रक्रिया की स्थापना करना ताकि संबंधित जोखिमों का पता लगाया जा सके और जोखिमों को कम करने के लिए आवश्यक नियंत्रण के उचित स्तर का निर्धारण किया जा सके।
- हडको आरबीआई/सेबी/भारत सरकार द्वारा जारी सरकारी दिशा-निर्देशों/नीतियों/कानूनों/ परिपत्रों/विनियमों आदि में उल्लिखित प्रासंगिक साइबर सुरक्षा और डेटा सुरक्षा/संरक्षण आवश्यकताओं को समझेगा, प्रबंधित करेगा और उनका अनुपालन करेगा, जैसे आईटी अधिनियम 2000, डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023 (डीपीडीपी अधिनियम 2023) या समय-समय पर जारी कोई अन्य कानून/परिपत्र/विनियम।

3. प्रबंधन

आईटी विभाग, सीआईएसओ के परामर्श से, सूचना एवं साइबर सुरक्षा नीति की वार्षिक समीक्षा करेगा और निदेशक मंडल के अनुमोदन के लिए प्रस्तुत करेगा।

4. नीति मानक और प्रक्रियाएँ

मानक विस्तृत आवश्यकताएँ जिन्हें साइबर सुरक्षा नीतियों के अनुपालन हेतु पूरा किया जाना आवश्यक है। प्रत्येक नीति वक्तव्य के लिए मानकों का एक अलग सेट विकसित किया जाना है। मानकों में वे उपाय शामिल हैं जो नीति वक्तव्यों द्वारा कवर किए गए संबंधित डोमेन से जुड़े सभी जोखिमों को कम करने के लिए किए जाने चाहिए। नीतियों और मानकों को कैसे लागू किया जाए, इस बारे में विस्तृत दिशानिर्देशों का दस्तावेजीकरण करने के लिए आवश्यकताओं के अनुसार अलग-अलग मानक संचालन प्रक्रियाएँ बनाई जानी हैं।

प्रक्रियाएं और दिशानिर्देश विकसित करने के मुख्य उद्देश्य हैं:

- यह सुनिश्चित करना कि साइबर सुरक्षा नीति और मानकों की व्याख्या हडको में सही और समान रूप से की जाए।
- नीति और मानकों के कार्यान्वयन के लिए दिशानिर्देश प्रदान करना।
- नीति और मानकों के बारे में जागरूकता बढ़ाना और उनके अनुपालन में सहायता करना और नीति का कार्यान्वयन चरणबद्ध तरीके से किया जाना है, जिसमें सबसे पहले महत्वपूर्ण गतिविधियों को प्राथमिकता दी जाएगी।

5. विस्तार

सूचना एवं साइबर सुरक्षा नीति निम्नलिखित पर लागू होती है:

- हडको के सभी कार्मिक, ठेकेदार, तृतीय पक्ष, आउटसोर्स भागीदार और कार्मिक।
- सभी सूचना परिसंपत्तियाँ जिनमें निम्नलिखित शामिल हैं, लेकिन इन्हीं तक सीमित नहीं हैं: सॉफ्टवेयर परिसंपत्तियां, हार्डवेयर परिसंपत्तियां, कागजी परिसंपत्तियां, सेवा परिसंपत्तियां, लोगों की परिसंपत्तियां और परिसंपत्तियां जो भौतिक या इलेक्ट्रॉनिक रूप से संग्रहीत, संसाधित और/या उपरोक्त किसी भी प्रकार की परिसंपत्ति द्वारा प्रेषित की जाती हैं।

6. अपवाद

सूचना और साइबर सुरक्षा नीति के विपरीत कार्य करने के ऐसे उदाहरण हो सकते हैं जहाँ उचित व्यावसायिक आवश्यकता हो। जब भी तकनीकी या व्यावसायिक कारणों से इस नीति का पालन करना संभव न हो, तो समयबद्ध छूट का अनुरोध किया जाना चाहिए। इस छूट को CISO द्वारा अनुमोदित किया जाना आवश्यक है। सभी अनुमोदित अपवादों की कम से कम वार्षिक रूप से या आवश्यकतानुसार समीक्षा की जानी चाहिए। व्याख्या से संबंधित किसी भी मुद्दे को सक्षम प्राधिकारी द्वारा अनुमोदित किया जाना चाहिए।

7. प्रवर्तन

न्यूनतम आवश्यकताओं का अनुपालन न करने या हडको सूचना एवं साइबर सुरक्षा नीति के उल्लंघन के परिणामस्वरूप निम्नलिखित कार्रवाई हो सकती है, लेकिन यह इन तक ही सीमित नहीं है:

- चेतावनी
- निलंबन
- उचित समझे जाने पर सिविल और/या आपराधिक मुकदमा
- हडको के सीडीए नियमों के अनुसार अन्य कार्रवाई।

8. साइबर सुरक्षा कौशलनीति

साइबर हमलों के जवाब में, हडको प्रबंधन ने अपनी आईटी संपत्तियों को साइबर हमलों से बचाने और किसी भी साइबर हमले या खतरे का समय पर और उचित तरीके से जवाब देने के लिए एक कौशलनीति बनाई है ताकि डेटा/आईटी प्रणालियों की गोपनीयता, अखंडता और उपलब्धता सुनिश्चित की जा सके। साइबर सुरक्षा कौशलनीति, जैसा कि चित्र 1 में दर्शाया गया है, पहचान, सुरक्षा, पता लगाना, प्रतिक्रिया, पुनर्प्राप्ति और सीखना है। नीचे दी गई तालिका हडको की साइबर सुरक्षा कौशलनीति के चरणों का चरण-वार विवरण प्रदान करती है।

क्रम सं.	स्तर	विवरण
1	पहचान	महत्वपूर्ण परिसंपत्तियों की पहचान और साइबर सुरक्षा जोखिमों का प्रबंधन
2	सुरक्षा	सुरक्षा वास्तुकला प्रणाली, घटना से जुडी सह-संबंध प्रणाली, घुसपैठ की रोकथाम एवं पता लगाने की प्रणाली, और सुरक्षित विन्यास के प्रवर्तन जैसे नियंत्रणों को तैनात करके लगातार पहचानी गई परिसंपत्तियों की सुरक्षा करना।
3	पता लगाना	महत्वपूर्ण बुनियादी ढांचे की निरंतर निगरानी के माध्यम से हमलों या विसंगतियों से संबंधित घटनाओं का पता लगाना।
4	प्रतिक्रिया	घटना के प्रभाव का आकलन करने हेतु कदम उठाएं और संबंधित प्राधिकारियों को सूचित करने के साथ साथ उचित प्रतिक्रिया उपाय करें।

5	पुनर्प्राप्ति	संगठन का घटना प्रबंधन, व्यवसाय निरंतरता और आपदा पुनर्प्राप्ति नीतियों और प्रक्रियाओं का पर्याप्त रूप से पालन करते हुए समय पर घटना से उबरना और यह सुनिश्चित करना कि गोपनीय डेटा का कोई नुकसान न हो और इसकी आईटी संपत्तियां साइबर हमलों से सुरक्षित रहें।
6	सीख	पुनर्प्राप्ति के बाद साइबर घटनाओं से प्रासंगिक सीखों को रिकॉर्ड करें और इस तरह की घटनाओं को रोकने के लिए योजना बनाएं।

9. सूचना सुरक्षा ढाँचा

यह नीति सूचना सुरक्षा से संबंधित प्रमुख मुद्दों की पहचान करती है और उनसे निपटने के लिए व्यापक दिशानिर्देश प्रदान करती है। इस नीति के आधार पर विस्तृत निर्देश और प्रक्रियाएँ विकसित की जाएँगी और उन पर कड़ी निगरानी आवश्यक होगी।

हडको, सूचना और साइबर सुरक्षा ढाँचे के प्रभावी कार्यान्वयन और रखरखाव को सुनिश्चित करने के लिए कार्यकारी स्तर पर कार्यरत सूचना सुरक्षा समिति (आईएससी) का गठन करेगा। आईएससी की कार्यवाई की जानकारी तिमाही आधार पर बोर्ड की आईटी कौशलनीति समिति को दी जाएगी।

10. जोखिम प्रबंधन

हडको एक मजबूत आईटी और सूचना सुरक्षा जोखिम प्रबंधन ढांचा स्थापित करेगा, जिसमें अन्य बातों के अलावा निम्नलिखित पहलुओं पर ध्यान दिया जाएगा:

- पहचाने गए जोखिमों को कम करने या प्रबंधित करने के लिए एक व्यापक सूचना सुरक्षा प्रबंधन कार्य का कार्यान्वयन, आंतरिक नियंत्रण और प्रक्रियाओं (लागू बीमा कवरेज सहित) । गतिशील रूप से बदलते जोखिम परिवेश से निपटने के लिए इन नियंत्रणों और प्रक्रियाओं की प्रभावशीलता की समय-समय पर समीक्षा की जानी चाहिए।
- आईटी जोखिम प्रबंधन में शामिल शेयरधारकों (तृतीय-पक्ष कर्मियों सहित) की भूमिकाओं और जिम्मेदारियों की परिभाषा। संभावित भूमिका संघर्षों और जवाबदेही के अंतरालों की विशिष्ट रूप से पहचान की जानी चाहिए और उनका उचित समाधान या प्रबंधन किया जाना चाहिए।
- संगठन की महत्वपूर्ण सूचना प्रणालियों की पहचान करना और इन प्रणालियों के आसपास सुरक्षा वातावरण को मजबूत करना; और
- डेटा और सूचना के सुरक्षित भंडारण, संचरण और प्रसंस्करण को सुनिश्चित करने के लिए आवश्यक प्रणालियों, प्रक्रियाओं और नियंत्रणों की परिभाषा और कार्यान्वयन।

10.1. सुरक्षा जोखिम मूल्यांकन

- हडको के विस्तार में प्रत्येक सूचना परिसंपत्ति के लिए जोखिम मूल्यांकन उचित सुरक्षा मानकों और आईटी नियंत्रण ढांचे द्वारा निर्देशित किया जाएगा।
- हडको यह सुनिश्चित करेगा कि सभी कर्मचारी सदस्य और सेवा प्रदाता उन पर लागू मौजूदा सूचना सुरक्षा और स्वीकार्य-उपयोग नीतियों का अनुपालन करें।

- हडको अपने सुरक्षा ढांचे और सुरक्षा नीतियों की कम से कम वार्षिक आधार पर समीक्षा करेगा, जिसमें अपने अनुभवों के साथ-साथ उभरते खतरों और जोखिमों पर भी विचार किया जाएगा। हडको फ़िशिंग और स्पूफिंग हमलों सहित साइबर हमलों से निपटने और उनके प्रतिकूल प्रभावों को कम करने के लिए उचित उपाय करेगा।
- सूचना सुरक्षा समिति को कम से कम वार्षिक आधार पर तथा पर्यावरण में कोई भी महत्वपूर्ण परिवर्तन करने से पहले सभी आईटी परिसंपत्तियों पर जोखिम मूल्यांकन की निगरानी करना आवश्यक है।
- हडको की प्राथमिकताएं, बाधाएं, जोखिम सहनशीलता और जोखिम उठाने की क्षमता संबंधी विवरण, धारणाएं और बाधाएं स्थापित की जाती हैं, संप्रेषित की जाती हैं और परिचालन जोखिम निर्णयों का समर्थन करने के लिए उनका उपयोग किया जाता है।
- जोखिम मूल्यांकन के भाग के रूप में निम्नलिखित गतिविधियाँ की जाएंगी:
    - जोखिम की पहचान - संभावित खतरों और उनके स्रोतों, कमजोरियों, सूचना परिसंपत्तियों पर प्रभाव के परिणामों एवं जोखिम स्वामियों की पहचान की जाती है।
    - जोखिम आकलन - व्यवसाय प्रभाव मूल्य, किसी घटना की संभावना (गुणात्मक या मात्रात्मक रूप से) का आकलन करना और जोखिम के स्तर का अनुमान लगाना।
    - जोखिम मूल्यांकन - जोखिम स्वीकृति या जोखिम उपचार मानदंडों के विरुद्ध जोखिम के स्तर की तुलना करना और जोखिम उपचार के लिए प्राथमिकता तय करना।

11. सूचना सुरक्षा का संगठन

11.1. आंतरिक संगठन

11.1.1. कर्तव्यों का पृथक्करण

सूचना परिसंपत्तियों के अनधिकृत या अनजाने संशोधन या दुरुपयोग के अवसरों को कम करने के लिए कर्तव्यों और जिम्मेदारी के क्षेत्रों को अलग-अलग किया जाएगा।

हडको की सूचना प्रणालियों के विकास, प्रसंस्करण, प्रशासन या प्रबंधन में भूमिका धारकों द्वारा निभाई जाने वाली जिम्मेदारियों की पहचान, दस्तावेजीकरण, अनुमोदन की आवश्यकता है और तदनुसार उपयोगकर्ताओं को अनुमोदित विशेषाधिकार प्रदान किए जाएंगे।

यह आवश्यक है कि उपयोगकर्ता खाता खोलने का अनुरोध और एक्सेस पात्रता अनुरोध, अनुरोधकर्ता द्वारा स्वयं अनुमोदित न हों। व्यवसाय प्रबंधक या उनके प्रतिनिधि अपनी एक्सेस पात्रताओं की समीक्षा या अनुमोदन नहीं कर सकते।

यह आवश्यक है कि परस्पर विरोधी भूमिकाओं और उपयोगकर्ताओं की पहचान की जाए। ऐसी परस्पर विरोधी भूमिकाओं का आवंटन अनुशंसित नहीं है। परस्पर विरोधी कर्तव्यों की एक सांकेतिक सूची निम्नलिखित है:

- एकल उपयोगकर्ता अपने स्वयं के लेनदेन को क्रियान्वित करने और अनुमोदित करने के लिए जिम्मेदार है, जैसे दोहरे नियंत्रण या 'मेकर-चेकर' का अभाव।

- अनुप्रयोग विकास/परीक्षण टीम, उत्पादन परिवेश में अनुप्रयोग प्रशासन का कार्य करती है।
- उपयोगकर्ता अपनी मशीनों के लिए लॉग निगरानी करते हैं; और
- सर्वर या नेटवर्क प्रशासक, डेटाबेस प्रशासन का कार्य करते हैं।
- नेटवर्क और सुरक्षा उपकरण का प्रबंधन एकल परिचालन टीम द्वारा किया जाता है।

जब किसी उपयोगकर्ता को परस्पर विरोधी भूमिकाएँ सौंपने की आवश्यकता होती है, तो निम्नलिखित नियंत्रणों का कार्यान्वयन आवश्यक है:

- अपवाद अनुरोध के लिए मान्य व्यावसायिक औचित्य का दस्तावेजीकरण किया जाता है।
- परस्पर विरोधी भूमिकाओं के कारण उत्पन्न होने वाले जोखिमों की पहचान की जाती है।
- ऐसी परस्पर विरोधी भूमिकाओं वाले उपयोगकर्ता आईडी लॉग किए जाते हैं।
- ऑडिट ट्रेल्स, अपवाद रिपोर्टिंग, समाधान और लेन-देन लॉग के माध्यम से गतिविधियों की निगरानी की जाती है।
- परस्पर विरोधी भूमिकाओं की समीक्षा संबंधित कार्यात्मक प्रमुखों द्वारा वर्ष में कम से कम एक बार की जाती है। परस्पर विरोधी भूमिकाओं को जारी रखने के लिए औपचारिक अनुमोदन वार्षिक समीक्षा के बाद प्राप्त किया जाएगा।

11.1.2. प्राधिकारी से संपर्क

यह आवश्यक है कि आपात स्थितियों से निपटने के लिए कानून प्रवर्तन प्राधिकारियों, नियामक निकायों, अग्निशमन विभाग, आपातकालीन सेवाओं और दूरसंचार प्रदाताओं सहित प्रासंगिक प्राधिकारियों के साथ उचित संपर्क बनाए रखा जाए।

11.1.3. विशेष रुचि समूहों से संपर्क

यह आवश्यक है कि विशेष रुचि समूहों या अन्य विशेषज्ञ सुरक्षा मंचों और प्रोफेसनल संघों के साथ उचित संपर्क बनाए रखा जाए। विशेष रुचि समूहों या सूचना सुरक्षा समिति मंचों की सदस्यता को निम्नलिखित के साधन के रूप में माना जाता है:

- अच्छी जानकारी अर्जित करके ज्ञान में सुधार करें और प्रासंगिक सुरक्षा जानकारी के साथ अद्यतित रहें।
- सुनिश्चित करें कि सूचना सुरक्षा परिवेश की समझ वर्तमान और पूर्ण है।
- पर्याप्त कौशल के साथ ज्ञान और कौशल को उन्नत करें।
- हमलों और कमजोरियों से संबंधित अलर्ट, सलाह और पैच की प्रारंभिक चेतावनियाँ प्राप्त करें।
- विशेषज्ञ सूचना सुरक्षा सलाह तक एक्सेस प्राप्त करें।
- सीआईएसओ और सीआईएसओ कार्यालय के कर्मचारी नवीनतम सुरक्षा खतरों, समाधानों आदि से अपडेट रहने के लिए मंचों/समूहों में शामिल हो सकते हैं।

11.2. मोबाइल उपकरण और टेलीवर्किंग

11.2.1. मोबाइल उपकरण नीति

- हडको द्वारा प्रबंधित मोबाइल डिवाइस जैसे स्मार्टफोन, टैबलेट, पीडीएस आदि में डिवाइस या हडको डेटा वाले एन्क्रिप्टेड कंटेनर पर मजबूत पासवर्ड सुरक्षा सक्षम होनी चाहिए।
- कार्मिकों को यह आवश्यक है कि जैसे ही उन्हें पता चले कि उनका डिवाइस खो गया है या चोरी हो गया है, वे 24 घंटे के भीतर अपने प्रबंधक या आईटी सहायता डेस्क को सूचित करें।
- उपयोगकर्ता मोबाइल उपकरणों पर इंटरनेट का उपयोग व्यावसायिक गतिविधियों के लिए करेंगे और गैर-व्यावसायिक गतिविधियों को प्रतिबंधित करेंगे या इंटरनेट सेवाओं के कभी-कभार और उचित व्यक्तिगत उपयोग की अनुमति देंगे।
- कर्मचारी केवल हडको द्वारा उपलब्ध कराई गई कनेक्टिविटी के माध्यम से ही इंटरनेट का उपयोग करेंगे तथा आईटी विभाग से अनुमति के बिना इंटरनेट का उपयोग नहीं करेंगे।
- हडको को अपने विवेकानुसार कुछ वेबसाइटों को फ़िल्टर करने और उनकी एक्सेस को प्रतिबंधित करने का अधिकार होगा।
- हडको इस नीति का अनुपालन सुनिश्चित करने के लिए उपयोगकर्ताओं के इंटरनेट उपयोग की निगरानी और समीक्षा करने का अधिकार सुरक्षित रखता है।
- उपयोगकर्ता अपने खाते से इंटरनेट एक्सेस के किसी भी दुरुपयोग के लिए जिम्मेदार होंगे।

11.2.2. टेलीवर्किंग

- हडको नेटवर्क तक दूरस्थ एक्सेस की अनुमति केवल तभी दी जाएगी जब कोई वैध व्यावसायिक की आवश्यकता हो और प्रबंधन की स्वीकृति के अधीन हो। यह आवश्यक है कि अंतिम उपयोगकर्ता वीपीएन एक्सेस का अनुरोध करें और रिपोर्टिंग प्रबंधक एवं आईटी विभाग से अपेक्षित अनुमोदन प्राप्त करें।
- हडको को यह सुनिश्चित करना चाहिए कि दूरस्थ एक्सेस उपयोगकर्ता अनुमोदित नीतियों का पालन करें।
- महत्वपूर्ण प्रणालियों तक उद्यम एक्सेस (तार्किक) के लिए बहु-कारक प्रमाणीकरण लागू करें।
- हडको की प्रणालियों से जुड़े/सभी रिमोट-एक्सेस उपकरणों की पहचान करने के लिए एक प्रणाली स्थापित करना तथा यह सुनिश्चित करना कि टेलीवर्किंग में साझा/प्रस्तुत किया गया डेटा/सूचना उचित रूप से सुरक्षित है।

12. कार्मिक सुरक्षा

मानव संसाधन सुरक्षा नीति का उद्देश्य मानवीय भूल, चोरी, धोखाधड़ी या सुविधाओं के दुरुपयोग के जोखिमों को कम करना है। हडको रोजगार की पुष्टि करने से पहले स्वतंत्र पहचान जाँच करेगा। स्वतंत्र पहचान जाँच, चयनित उम्मीदवारों के हडको में शामिल होने के स्तर को ध्यान में रखते हुए की जाएगी।

12.1 रोजगार की शर्तें और नियम

प्रत्येक नए कर्मचारी को प्रवेश प्रक्रिया के दौरान और सत्रों के माध्यम से सुरक्षा भूमिकाओं और जिम्मेदारियों के बारे में स्पष्ट रूप से बताया जाना चाहिए।

मानव संसाधन विभाग को यह सुनिश्चित करना होगा कि 'रोजगार की शर्तें और नियम' सूचना सुरक्षा आवश्यकताओं को प्रतिबिंबित करें और निम्नलिखित बिंदुओं को भी शामिल किया जाना आवश्यक है:

- सभी कर्मचारियों के लिए गोपनीयता समझौते पर हस्ताक्षर करना अनिवार्य होने के कारण, वे सूचना के किसी भी अनधिकृत प्रकटीकरण, संशोधन और/या विनाश के लिए उत्तरदायी होंगे।
- सूचना की गोपनीयता और अखंडता बनाए रखने की जिम्मेदारी।
- यदि कोई उपयोगकर्ता हडको सुरक्षा ढांचे की आवश्यकताओं की अवहेलना करता है तो कार्रवाई की जाएगी।
- रोजगार समाप्ति के बाद भी हडको की सूचना की गोपनीयता की सुरक्षा के लिए कर्मचारी की जिम्मेदारियों का जारी रहना।
- किसी भी कार्मिक द्वारा किसी भी प्रकार की सूचना सुरक्षा भंग किए जाने पर, जो हानिकारक प्रकृति की हो, उसे तत्काल सेवा से हटा दिया जाएगा।

12.2 सूचना सुरक्षा जागरूकता, शिक्षा और प्रशिक्षण

प्रबंधन को सूचना सुरक्षा और हडको सूचना संसाधनों की सुरक्षा के संबंध में उन सभी कार्मिकों के लिए सतत जागरूकता और प्रशिक्षण कार्यक्रम उपलब्ध कराने की आवश्यकता है, जिनके कर्तव्यों के कारण उन्हें गोपनीय या संवेदनशील सूचना संसाधनों के संपर्क में आना पड़ता है।

यह आवश्यक है कि हडको के कार्मिक अपनी सूचना सुरक्षा जिम्मेदारियों को स्वीकार करें।

उपयोगकर्ता प्रशिक्षण का उद्देश्य यह सुनिश्चित करना है कि उपयोगकर्ता सूचना सुरक्षा खतरों और चिंताओं से अवगत हों तथा अपने सामान्य कार्य के दौरान संगठनात्मक सुरक्षा नीति का समर्थन करने के लिए तैयार हों।

- सूचना और साइबर सुरक्षा नीतियों के बारे में जागरूकता सुनिश्चित करने के लिए, सभी कार्मिकों, विक्रेताओं, सेवा प्रदाताओं और शेयरधारकों को उनकी भूमिकाओं, ज़िम्मेदारियों और गैर-अनुपालन के संभावित परिणामों के बारे में सूचित किया जाएगा। विभाग यह सुनिश्चित करेंगे कि संबंधित कार्मिक साइबर सुरक्षा ढाँचे की प्रभावशीलता में अपने योगदान को समझें।

- अनुपालन और सुरक्षा उद्देश्यों के महत्व को सुदृढ़ करने के लिए सक्षम प्राधिकारी सहित सभी कार्मिकों के लिए प्रतिवर्ष साइबर सुरक्षा जागरूकता सत्र आयोजित किए जाएंगे।

- हडको ग्राहकों को वर्तमान ऑनलाइन और मोबाइल बैंकिंग खतरों के बारे में शिक्षित करना, फीडबैक एकत्र करना, तथा समय-समय पर उन्हें उभरते साइबर जोखिमों के बारे में अद्यतन करना, तथा किसी भी साइबर हमले की रिपोर्टिंग के लिए प्रोत्साहित करना।
- ऑनलाइन और ऑफलाइन साइबर सुरक्षा जागरूकता अभियान शुरू करें ताकि ग्राहकों को तीसरे पक्ष के विक्रेताओं के साथ संवेदनशील हडको क्रेडेंशियल्स (जैसे, लॉगिन, पासवर्ड, पिन) साझा करने के जोखिमों के बारे में सूचित किया जा सके।

13. परिसंपत्ति प्रबंधन

परिसंपत्ति प्रबंधन, परिसंपत्ति स्वामी की पहचान और परिसंपत्ति वर्गीकरण सहित प्रत्येक सूचना परिसंपत्ति के रिकॉर्ड बनाए रखने के महत्व को निर्दिष्ट करता है।

हडको की सूचना परिसंपत्तियों को व्यापक सुरक्षा प्रदान की जाएगी और उनका एक निश्चित स्वामी होगा। इसमें यह सुनिश्चित करने के निर्देश दिए गए हैं कि:

- प्रत्येक व्यावसायिक कार्य की सूचना परिसंपत्तियों के प्रकारों का दस्तावेजीकरण करने के लिए एक सूचना परिसंपत्ति रजिस्टर बनाया है।
- प्रत्येक व्यावसायिक कार्य की सूचना परिसंपत्तियों के लिए नामित स्वामी होते हैं
- डेटा, कार्मिक, उपकरण, प्रणालियाँ और सुविधाएँ जो हडको को अपने व्यावसायिक उद्देश्यों को प्राप्त करने में सक्षम बनाती हैं, उनकी संगठनात्मक उद्देश्यों और हडको की जोखिम कौशलनीति के लिए उनके सापेक्ष महत्व के अनुसार लगातार पहचान और प्रबंधन किया जाता है।
- भौतिक उपकरण, डिजिटल परिसंपत्तियां (जैसे यूआरएल, डोमेन नाम, एप्लिकेशन, एपीआई, आदि), साझा संसाधन (क्लाउड परिसंपत्तियां सहित) और संगठन के भीतर अन्य इंटरफेसिंग प्रणालियों की समयबद्ध तरीके से सूची बनाई जाती है।
- संगठनात्मक संचार, डेटा प्रवाह और एन्क्रिप्शन विधियों को सभी आईटी प्रणालियों और नेटवर्क संसाधनों के संबंध में मैप और सूचीबद्ध किया जाएगा।
- हडको यह सुनिश्चित करेगा कि संगठन में कोई छाया आईटी (shadow IT) परिसंपत्तियां मौजूद न हों।
- डेटा की सूची, तथा निर्दिष्ट डेटा प्रकारों के लिए संगत मेटाडेटा बनाए रखा जाता है।

13.1. परिसंपत्तियों का प्रबंधन

हडको को व्यवसायिक कार्य से जुड़ी सभी सूचना परिसंपत्तियों की अद्यतन सूची तैयार करने तथा वर्गीकरण दिशानिर्देश निर्धारित करने की आवश्यकता है।

13.1.1 परिसंपत्तियों की सूची

हडको उन परिसंपत्तियों की एक सूची बनाएगा जिनका उपयोग सूचना प्रसंस्करण के लिए किया जाता है, जिसमें सूचना स्वयं भी शामिल है, ताकि यह सुनिश्चित किया जा सके कि इन परिसंपत्तियों की प्रभावी सुरक्षा सुनिश्चित हो। परिसंपत्तियों को चार प्रमुख समूहों में वर्गीकृत किया जाएगा:

- **सूचना परिसंपत्ति -** डेटाबेस और डेटा फ़ाइलें (स्थानीय डेस्कटॉप/लैपटॉप में महत्वपूर्ण डेटा सहित), सिस्टम दस्तावेजीकरण, उपयोगकर्ता दस्तावेजीकरण, प्रशिक्षण सामग्री, परिचालन/समर्थन प्रक्रियाएं, निरंतरता योजनाएं, संग्रहीत जानकारी, लाइसेंस आदि शामिल होंगे। सूचना परिसंपत्ति को आगे दो प्रारूपों में उपवर्गीकृत किया जा सकता है - इलेक्ट्रॉनिक और पेपर प्रारूप।

- **सॉफ्टवेयर परिसंपत्ति -** इसमें एप्लीकेशन सॉफ्टवेयर, सिस्टम सॉफ्टवेयर, विकास उपकरण और उपयोगिताएं आदि शामिल होंगी।
- **हार्डवेयर परिसंपत्ति -** इसमें कंप्यूटर उपकरण (सर्वर, डेस्कटॉप, लैपटॉप, मोडेम, प्रिंटर आदि), संचार उपकरण (नेटवर्क डिवाइस), अप्रयुक्त चुंबकीय मीडिया (टेप आदि) शामिल होंगे।
- **सेवा परिसंपत्ति -** इसमें सामान्य उपयोगिता सेवाएं जैसे बिजली, प्रकाश व्यवस्था और एयर कंडीशनिंग आदि शामिल होंगी।
- **मुख्य कार्मिक -** इसमें किसी अन्य परिसंपत्ति को समर्थन देने और लागू करने ने हेतु मुख्य कार्मिक शामिल होंगे।
- प्रत्येक परिसंपत्ति का एक नामित स्वामी होगा और उचित नियंत्रणों के रखरखाव की ज़िम्मेदारी उसको सौंपी जाएगी। सभी चार प्रकार की परिसंपत्तियों के लिए इन्वेंट्री रजिस्टर बनाए जाएँगे और इन्वेंट्री रजिस्टरों की सटीकता सुनिश्चित करने के लिए इन्वेंट्री की समय-समय पर समीक्षा की जाएगी।
- सभी सूचना परिसंपत्तियों को सूचना परिसंपत्ति रजिस्टर में लिखा जाना आवश्यक है ।

13.1.2 परिसंपत्तियों का स्वामित्व

- सभी सूचना परिसंपत्तियों के लिए एक निर्दिष्ट स्वामी होना आवश्यक है। परिसंपत्ति स्वामी उन अधिकृत उपयोगकर्ताओं की पहचान करने के लिए ज़िम्मेदार होगा जो सूचना परिसंपत्ति तक एक्सेस कर सकते हैं।
- सूचना परिसंपत्तियों को उनके व्यावसायिक मूल्य और व्यावसायिक संचालन पर प्रभाव के आधार पर वर्गीकृत किया जाएगा।
- सूचना परिसंपत्ति रजिस्टर की समीक्षा वर्ष में कम से कम एक बार की जानी चाहिए, या कोई महत्वपूर्ण परिवर्तन हो सकता है।

13.1.3 परिसंपत्तियों का स्वीकार्य उपयोग

- हडको कार्मिक अपनी यूजर आईडी से जुड़ी सभी गतिविधियों के लिए जवाबदेह हैं।
- हडको संसाधनों का उपयोग व्यावसायिक उद्देश्यों तक सीमित है और हडको इस उपयोग की निगरानी और रिपोर्ट करने का अधिकार सुरक्षित रखता है।
- हडको द्वारा प्रबंधित संसाधनों का उपयोग हडको के व्यावसायिक उद्देश्यों से संबंधित गतिविधियों के अलावा अन्य वाणिज्यिक गतिविधियों के लिए निषिद्ध है।
- हडको द्वारा उपलब्ध कराए गए कंप्यूटिंग और नेटवर्क संसाधनों का उपयोग केवल अधिकृत कर्मचारियों और तृतीय पक्षों द्वारा ही किया जा सकता है।
- हडको प्रौद्योगिकी संसाधनों के निम्नलिखित उपयोग अस्वीकार्य माने जाएंगे:

- व्यक्तिगत उपयोग के लिए कार्यालय से सूचना प्रेषित करना या हटाना, जो ग्राहकों और हडको कार्मिकों की गोपनीयता और हडको बौद्धिक संपदा का उल्लंघन करता है।
- कंप्यूटर संसाधनों को ख़राब करना या अन्य उपयोगकर्ताओं को बाहर करके उन संसाधनों पर एकाधिकार करना।
- किसी भी सिस्टम पर उपयोगकर्ता प्रमाणीकरण या प्राधिकरण को रद्द करना।
- बिना लाइसेंस वाले/गैर-अनुमोदित/क्रैक किए गए सॉफ़्टवेयर, डेटा और हार्डवेयर को स्थापित करना और/या उपयोग करना।
- किसी भी अस्वीकृत हार्डवेयर को हडको नेटवर्क से जोड़ना।
- किसी भी परिस्थिति में हडको का कोई भी कार्मिक हडको के स्वामित्व वाले संसाधनों का उपयोग करते समय किसी भी ऐसी गतिविधि में शामिल नहीं होगा जो कॉर्पोरेट, स्थानीय, राज्य, राष्ट्रीय या अंतर्राष्ट्रीय कानूनों के तहत अवैध है।
- कॉपीराइट, व्यापार गोपनीयता, पेटेंट या अन्य बौद्धिक संपदा, या समान कानूनों या विनियमों द्वारा संरक्षित किसी भी व्यक्ति या कंपनी के अधिकारों का उल्लंघन, जिसमें "पायरेटेड" या अन्य सॉफ्टवेयर उत्पादों की स्थापना या वितरण शामिल है, लेकिन यह इन्हीं तक सीमित नहीं है, जिन्हें हडको द्वारा उपयोग के लिए उचित रूप से लाइसेंस नहीं दिया गया है।
- कॉपीराइट सामग्री की अनधिकृत प्रतिलिपि बनाना, जिसमें पत्रिकाओं, पुस्तकों या अन्य कॉपीराइट स्रोतों से तस्वीरों का डिजिटलीकरण और वितरण, कॉपीराइट संगीत, और किसी भी कॉपीराइट सॉफ्टवेयर की स्थापना शामिल है, लेकिन यह इन्हीं तक सीमित नहीं है, जिसके लिए संगठन या अंतिम उपयोगकर्ता के पास कोई सक्रिय अधिकार नहीं है।
- अंतर्राष्ट्रीय या राष्ट्रीय निर्यात नियंत्रण कानूनों का उल्लंघन करते हुए सॉफ़्टवेयर, तकनीकी जानकारी, एन्क्रिप्शन सॉफ़्टवेयर या तकनीक का निर्यात/आयात करना अवैध है। किसी भी संदिग्ध सामग्री के निर्यात/आयात से पहले उपयुक्त प्रबंधन से परामर्श करना आवश्यक है।
- नेटवर्क या सर्वर में दुर्भावनापूर्ण प्रोग्राम या स्पाइवेयर, प्रॉक्सी बाईपास टूल आदि का प्रवेश (जैसे, वायरस, वर्म्स, ट्रोजन हॉर्स, ई-मेल बम, आदि) जो संगठन के लिए कोई संभावित खतरा पैदा कर सकते हैं।
- असुरक्षित इंटरनेट उपकरणों के उपयोग से जुड़े जोखिमों को देखते हुए, इंटरनेट डेटा कार्ड, ब्रॉडबैंड कनेक्शन या इंटरनेट कनेक्टिविटी की अन्य प्रणालियों के उपयोग (प्राधिकृत एंटरप्राइज़ इंटरनेट सेटअप के उपयोग को छोड़कर) को संगठन के परिसर में और संगठन के एंटरप्राइज़ सिस्टम पर उपयोग करने से प्रतिबंधित किया जाता है और इस नीति का उल्लंघन करने वाले कार्मिकों पर अनुशासनात्मक कार्रवाई की जाएगी।
- अन्य गतिविधियाँ जिन्हें मानव संसाधन या समान कार्य द्वारा अस्वीकार्य और अवैध माना जाता है।

- यह आवश्यक है कि हडको के आंतरिक नेटवर्क को संग्रहीत करने, संचारित करने और/या उससे कनेक्ट करने के लिए केवल हडको द्वारा प्रबंधित प्रौद्योगिकी संसाधनों (जैसे डेस्कटॉप, लैपटॉप) का ही उपयोग किया जाए।

- हडको नेटवर्क से कनेक्ट करने के लिए गैर-हडको प्रबंधित प्रौद्योगिकी संसाधनों का उपयोग करने से पहले सूचना यह आवश्यक है कि सुरक्षा समिति से औपचारिक अनुमोदन प्राप्त किया जाए।
- जहां अनुमोदन प्राप्त हो चुका है, वहां हडको नेटवर्क से जुड़ने के लिए उपयोग किए जाने वाले गैर-हडको प्रबंधित प्रौद्योगिकी संसाधन हडको की निम्नलिखित सुरक्षा आवश्यकताओं के अधीन हैं:
    - वायरस और अन्य मैलवेयर
    - मोबाइल डिवाइस
    - वायरलेस नेटवर्क
    - एकीकृत संचार
    - संदेश और इंटरनेट का उपयोग
- हडको की संवेदनशील जानकारी को कार्यालय से बाहर ले जाने से पहले, निम्नलिखित पर विचार किया जाएगा:
    - सूचना की संवेदनशीलता
    - सूचना के नुकसान या प्रकटीकरण का संभावित प्रभाव
    - हानि या प्रकटीकरण से बचने के लिए आवश्यक सावधानियां
    - उपयोगकर्ताओं को हडको द्वारा प्रबंधित प्रौद्योगिकी संसाधनों, जिनका उपयोग हडको की जानकारी संग्रहीत करने के लिए किया जाता है, के नुकसान की सूचना तुरन्त आईटी विभाग को देनी होगी।
- संवेदनशील हडको सूचना को सुरक्षित करने के लिए एन्क्रिप्शन या समकक्ष सुरक्षा पद्धति का उपयोग तब किया जाएगा जब:
    - इंटरनेट पर प्रसारित गैर-कॉर्पोरेट नेटवर्क ।
    - मोबाइल डिवाइस और हटाने योग्य मीडिया पर संग्रहीत।
- उपयोगकर्ता अपने डेस्कटॉप, लैपटॉप और अन्य मोबाइल उपकरणों को बिना निगरानी के छोड़ने से पहले उन्हें लॉक कर देंगे। उपयोगकर्ताओं को इस बात का पूरा ध्यान रखना चाहिए कि वे किसी भी ऐसे मोबाइल उपकरण को बिना निगरानी के न छोड़ें जिसमें संगठन का डेटा/ईमेल हो।
- बिजली की खपत बचाने के लिए उपयोगकर्ताओं को कार्यदिवस के अंत में डेस्कटॉप/लैपटॉप बंद कर देने चाहिए।

13.2. सूचना वर्गीकरण

13.2.1 सूचना का वर्गीकरण

सभी जानकारी निम्नलिखित सूचना वर्गीकरण श्रेणियों के अनुसार संरक्षित की जाएगी:

- **सार्वजनिक:** संबंधित विभाग द्वारा यह जानकारी सार्वजनिक रूप से जारी करने के लिए विशेष रूप से अनुमोदित की गई है। इस जानकारी के अनधिकृत प्रकटीकरण से हडको को अपने ग्राहकों या अपने व्यावसायिक भागीदारों के लिए कोई समस्या नहीं होनी चाहिए।। उदाहरण: हडको के इंटरनेट वेब पेज पर पोस्ट किए गए मार्केटिंग ब्रोशर और सामग्री। डको की जानकारी को सार्वजनिक रूप से प्रकट करने के लिए इस लेबल का होना, जानकारी के स्वामी की विशिष्ट अनुमति, या इस जानकारी को सार्वजनिक रूप से वितरित करने की दीर्घकालिक प्रचालन आवश्यक है।

- **आंतरिक:** यह जानकारी हडको के भीतर और कुछ मामलों में हडको के व्यावसायिक भागीदारों जैसे संबद्ध संगठनों के उपयोग के लिए है। बाहरी लोगों को इस जानकारी का अनधिकृत प्रकटीकरण कानूनों और नियमों के विरुद्ध हो सकता है, या हडको, उसके ग्राहकों या उसके व्यावसायिक भागीदारों के लिए समस्याएँ बढ़ा सकता है।

- **गोपनीय:** यह जानकारी निजी या अन्यथा संवेदनशील प्रकृति की है और यह आवश्यक है कि यह जानकारी केवल उन्हीं लोगों तक सीमित रहे जिन्हें इसकी एक्सेसच की वैध व्यावसायिक आवश्यकता है। जिन लोगों को इसकी पहुँच की व्यावसायिक आवश्यकता नहीं है, उनके लिए इस जानकारी का अनधिकृत प्रकटीकरण कानूनों और विनियमों के विरुद्ध हो सकता है, या हुडको, उसके ग्राहकों या उसके व्यावसायिक भागीदारों के लिए गंभीर समस्याएँ बढ़ा सकता है।

- **महत्वपूर्ण:** यह जानकारी अत्यंत निजी या अन्यथा संवेदनशील है और इस पर हर समय कड़ी निगरानी और नियंत्रण की आवश्यकता है। बिना व्यावसायिक आवश्यकता वाले लोगों को इस जानकारी का अनधिकृत प्रकटीकरण कानूनों और नियमों के विरुद्ध हो सकता है, या हडको, उसके ग्राहकों या उसके व्यावसायिक भागीदारों के लिए गंभीर समस्याएँ बढ़ा सकता है।

13.2.2 सूचना का लेबलिंग

यह आवश्यक है कि सूचना लेबलिंग के लिए प्रक्रियाओं का एक उपयुक्त सेट विकसित किया जाए और हडको द्वारा अपनाई गई सूचना वर्गीकरण योजना के अनुसार कार्यान्वित किया जाए। सूचना स्वामियों को यह निर्धारित करने के लिए सूचना वर्गीकरण श्रेणियों की समीक्षा करनी होगी कि सूचना को गोपनीय बनाया जाना है या नहीं।

13.2.3 सूचना का प्रबंधन

- कागज़ के रूप में सभी गोपनीय और महत्वपूर्ण दस्तावेज़ों को ताले में बंद रखा जाएगा। इलेक्ट्रॉनिक रूप में ऐसी किसी भी जानकारी को, जहाँ तक संभव हो, तकनीकी नियंत्रण द्वारा संरक्षित किया जाएगा।
- महत्वपूर्ण दस्तावेज़ का उपयोग करने के लिए एक्सेस सूची दस्तावेज़ स्वामी को ज्ञात होनी चाहिए।
- किसी भी दस्तावेज़ को मुद्रित या स्कैन किए जाने पर उसे तुरन्त प्रिंटर या स्कैनर से हटा दिया जाएगा।
- सभी सिस्टम दस्तावेज़ों को सुरक्षित जगह में संग्रहीत किया जाएगा और अनधिकृत एक्सेस से भौतिक रूप से संरक्षित किया जाएगा।
- सिस्टम दस्तावेज़ीकरण की वितरण सूची पूरी तरह से 'जानने की आवश्यकता' के आधार पर है और संबंधित सूचना परिसंपत्ति स्वामी द्वारा अधिकृत है।

13.3. बैकअप मीडिया

कंपनी के महत्वपूर्ण डेटा की सुरक्षा और पुनर्प्राप्ति सुनिश्चित करने के लिए, नियमित डेटा बैकअप हेतु बैकअप मीडिया का उपयोग किया जाएगा। निम्नलिखित प्रक्रियाओं का पालन किया जाएगा:

1. **बैकअप मीडिया का चयन:** कंपनी बैकअप किए जा रहे डेटा के प्रकार और मात्रा के आधार पर विश्वसनीय और सुरक्षित बैकअप मीडिया का उपयोग करेगी, जिसमें बाह्य हार्ड ड्राइव, क्लाउड स्टोरेज और अन्य उपयुक्त तरीके शामिल होंगे।
2. **बैकअप शेड्यूल:** डेटा बैकअप एक नियमित शेड्यूल (जैसे, दैनिक, साप्ताहिक) पर किया जाएगा, जैसा कि व्यावसायिक आवश्यकताओं और डेटा की गंभीरता द्वारा निर्धारित किया जाएगा।
3. **डेटा एन्क्रिप्शन और सुरक्षा:** डेटा की गोपनीयता और अनधिकृत एक्सेस से सुरक्षा सुनिश्चित करने के लिए सभी बैकअप मीडिया को एन्क्रिप्ट किया जाएगा। बैकअप डेटा को, जहाँ भी लागू हो, ऑन-साइट और ऑफ-साइट दोनों जगह सुरक्षित रूप से संग्रहीत किया जाएगा।
4. **परीक्षण और सत्यापन:** बैकअप की अखंडता और प्रभावशीलता सुनिश्चित करने के लिए बैकअप सिस्टम और डेटा पुनर्स्थापना प्रक्रियाओं का नियमित परीक्षण किया जाएगा।
5. **अवधारण और निपटान:** बैकअप डेटा को कंपनी की अवधारण नीतियों के अनुसार बनाए रखा जाएगा, और अनधिकृत एक्सेस को रोकने के लिए पुराने या अनावश्यक बैकअप को सुरक्षित रूप से नष्ट कर दिया जाएगा।
6. **जिम्मेदारी:** नामित कार्मिक बैकअप प्रक्रिया की देखरेख, समय पर निष्पादन सुनिश्चित करने और बैकअप मीडिया के साथ उत्पन्न होने वाली किसी भी समस्या का समाधान करने के लिए जिम्मेदार होंगे।
7. यह बैकअप मीडिया कार्यान्वयन डेटा हानि के जोखिम को कम करने और आपात स्थिति में व्यावसायिक निरंतरता सुनिश्चित करने के लिए डिज़ाइन किया गया है। सुनिश्चित करें कि ईआरपी बैकअप की प्रतियाँ अग्निरोधी अलमारी/तिजोरी में भौतिक रूप से रखी गई हों।

13.4. मीडिया हैंडलिंग

13.4.1 रिमूवेबल मीडिया का प्रबंधन

हडको रिमूवेबल मीडिया को संबंधित विभाग के प्रमुख की स्पष्ट अनुमति के बिना ऐसे कंप्यूटरों से नहीं जोड़ा जाएगा जो संगठन के स्वामित्व में नहीं हैं या पट्टे पर नहीं हैं।

गोपनीय और महत्वपूर्ण डेटा जो कि यूएसबी डिवाइस, पोर्टेबल हार्ड ड्राइव, चुंबकीय टेप जैसे हटाने योग्य मीडिया पर संग्रहीत है, उसे हडको द्वारा अनुमोदित एन्क्रिप्शन प्रौद्योगिकियों का उपयोग करके एन्क्रिप्ट किया जाएगा।

अनुमत अपवाद प्रक्रियाओं के तहत, मामले-दर-मामला आधार पर इस नीति के अपवादों का अनुरोध किया जा सकता है। इस नीति का उल्लंघन करने वाले किसी भी कर्मचारी पर अनुशासनात्मक कार्रवाई की जा सकती है।

हडको हटाने योग्य मीडिया (जैसे यूएसबी, बाहरी हार्ड डिस्क, आदि) और इलेक्ट्रॉनिक उपकरणों (जैसे लैपटॉप, मोबाइल डिवाइस, आदि) के प्रतिबंध और सुरक्षित उपयोग के लिए नीति को परिभाषित और कार्यान्वित करेगा।

13.4.2 मीडिया का निराकरण

महत्वपूर्ण और गोपनीय जानकारी के साथ-साथ लाइसेंस प्राप्त सॉफ्टवेयर का निराकरण या पुनः उपयोग से पहले कंप्यूटर उपकरण और हटाने योग्य मीडिया से हटा दिया जाएगा।

जब तक यह पुष्टि न कर ली जाए कि डेटा हडको द्वारा परिभाषित अवधारण अवधि के अंत तक पहुंच गया है और कोई अतिरिक्त अवधारण अवधि (जैसे मुकदमेबाजी रोक या संरक्षण नोटिस) नहीं है। तब तक डेटा का निपटान या विनाश निषिद्ध है ।

निपटान के सुरक्षित तरीके, जैसे पोंछना, डीगॉसिंग या भौतिक विनाश, स्वीकार्य हैं जिसकी निम्नलिखित प्रक्रियाएँ हैं:

- हार्ड डिस्क: ऊपर उल्लेखित क्षमता वाले उपकरणों का उपयोग करके डेटा को अधिलेखित किया जाना है।
- टेप: नष्ट करें - विघटित करें, चूरा करें, या टुकड़े-टुकड़े करें।
- सीडी-आरओएम: नष्ट करें - विघटित करें, चूरा करें, या टुकड़े-टुकड़े करें।
- यूएसबी ड्राईवर: नष्ट करें - विघटित करें, चूरा करें, या टुकड़े-टुकड़े करें।
- सभी गैर-पुनर्लेखन योग्य भंडारण माध्यम (अर्थात, एक बार लिखें, लिखने के बाद केवल पढ़ें): नष्ट करें - विघटित करें, चूरा करें, या टुकड़े-टुकड़े करें।

13.4.3 भौतिक मीडिया स्थानांतरण

गोपनीय और महत्वपूर्ण डेटा, जो हटाने योग्य मीडिया (जैसे टेप, यूएसबी, आदि) पर भेजा जाता है, हडको द्वारा अनुमोदित एन्क्रिप्शन विधियों का उपयोग करके एन्क्रिप्ट किया जाएगा। जहाँ एन्क्रिप्शन तकनीकी रूप से संभव नहीं है, वहाँ यह सुनिश्चित किया जाएगा कि ऐसे मीडिया को हडको के अधिकृत कार्मिक द्वारा व्यक्तिगत रूप से/सुरक्षित तरीके से ले जाया जाए। परिवहन स्थल पर परिवहन का रिकॉर्ड रखा जाना चाहिए।

14. एक्सेस नियंत्रण

- सूचना परिसंपत्तियों तक एक्सेस केवल तभी दी जाएगी जब कोई वैध व्यावसायिक आवश्यकता हो। हडको के पास प्रलेखित मानक और प्रक्रियाएँ होंगी, जिन्हें आईटीएससी द्वारा अनुमोदित किया जाएगा और सूचना प्रणाली तक आवश्यकता-आधारित एक्सेस के प्रबंधन के लिए अद्यतन रखा जाएगा।
- अच्छे सिस्टम एक्सेस अधिकार वाले कार्मिकों की बारीकी से निगरानी तथा उनकी सभी सिस्टम गतिविधियों को लॉग करने एवं समय-समय पर उनकी समीक्षा की जाएगी।
- हडको को विशेषाधिकार प्राप्त उपयोगकर्ताओं के लिए बहु-कारक प्रमाणीकरण अपनाना होगा
  i) महत्वपूर्ण सूचना प्रणालियाँ
  ii) महत्वपूर्ण गतिविधियों के लिए, हडको के जोखिम मूल्यांकन के आधार पर।

- अनधिकृत तार्किक एक्सेस के विरुद्ध सूचना परिसंपत्तियों की सुरक्षा के लिए जोखिम के अनुसार सभी हडको आईटी सिस्टम के लिए एक्सेस नियंत्रण आवश्यक है।

14.1. एक्सेस कंट्रोल की व्यावसायिक आवश्यकता

14.1.1 एक्सेस नियंत्रण का प्रबंधन

- प्रबंधक अपने पर्यवेक्षण के अंतर्गत उपयोगकर्ताओं के एक्सेस अधिकारों के लिए जवाबदेह होंगे।

- उपयोगकर्ताओं को किसी विशेष भूमिका या कार्य के लिए आवश्यक न्यूनतम विशेषाधिकार प्रदान किए जाएंगे।
- विशेष विशेषाधिकार खातों के लिए अतिरिक्त प्रतिबंध लागू किए जाएंगे।
- सभी एक्सेस की आवधिक आधार पर समीक्षा की जाएगी और उचित कार्रवाई की जाएगी।
- उपयोगकर्ताओं को दूरस्थ रूप से कनेक्ट करने की अनुमति देते समय अतिरिक्त प्रमाणीकरण विधियों (जैसे दो कारक प्रमाणीकरण) का उपयोग किया जाएगा।
- ऑपरेटिंग सिस्टम तक एक्सेस को सुरक्षित लॉगऑन प्रक्रिया द्वारा नियंत्रित किया जाएगा।
- ऐसे उपयोगिता कार्यक्रमों का उपयोग, जो सिस्टम और अनुप्रयोग नियंत्रणों को ओवरराइड करने में सक्षम हो सकते हैं, प्रतिबंधित और कड़े नियंत्रण में रखा जाएगा।
- उच्च जोखिम वाले अनुप्रयोगों के लिए अतिरिक्त सुरक्षा प्रदान करने हेतु कनेक्शन के समय पर प्रतिबंध का उपयोग किया जाएगा।
- निष्क्रिय सत्रों को निष्क्रियता की एक निर्धारित अवधि के बाद समाप्त कर दिया जाएगा।

14.1.2 नेटवर्क और नेटवर्क सेवाओं तक एक्सेस

- हडको की महत्वपूर्ण आईटी परिसंपत्तियों और उच्च जोखिम (इंटरनेट से संबंधित) से प्रभावित परिसंपत्तियों को अलग करने के लिए कंप्यूटर नेटवर्क को अलग किया जाएगा।
- संवेदनशील सिस्टमों को समर्पित (पृथक) कंप्यूटिंग वातावरण होगा।
- कोई भी श्रेणी/वेबसाइट जो सुरक्षा जोखिम उत्पन्न करती है, उसे उचित जांच के बाद स्पष्ट रूप से ब्लॉक कर दिया जाएगा।
- गैर-व्यावसायिक संबंधित वेबसाइट जैसे पोर्नोग्राफी, आतंकवाद, हैकिंग और धार्मिक उत्तेजक साइटों आदि तक एक्सेस प्रतिबंधित होगी।

14.1.3 एडवांस्ड वास्तविक खतरा रक्षा और प्रबंधन

सम्पूर्ण भारत में हडको के नेटवर्क और विदेशी कार्यालयों के लिए खतरे के परिदृश्य की वास्तविक समय निगरानी के माध्यम से सूचना की सुरक्षा सुनिश्चित करना।

- हडको उद्यम में कई बिंदुओं पर दुर्भावनापूर्ण कोड की स्थापना, प्रसार और निष्पादन के विरुद्ध एक मजबूत सुरक्षा तंत्र का निर्माण करेगा।
- हडको सभी श्रेणियों के उपकरणों (एंडपॉइंट जैसे पीसी/लैपटॉप/मोबाइल डिवाइस आदि), सर्वर (ऑपरेटिंग सिस्टम, डेटाबेस, एप्लिकेशन आदि), वेब/इंटरनेट गेटवे, ईमेल-गेटवे, वायरलेस नेटवर्क, एसएमएस सर्वर आदि के लिए व्यवहार पहचान प्रणालियों सहित एंटी-मैलवेयर, एंटीवायरस सुरक्षा को लागू करेगा, जिसमें केंद्रीकृत प्रबंधन और निगरानी के लिए उपकरण और प्रक्रियाएं शामिल हैं।
- व्यावसायिक संचालन के लिए आवश्यक अधिकृत वेबसाइटों की एक श्वेतसूची परिभाषित और अनुरक्षित की जाएगी।

- वेब/इंटरनेट गेटवे से गुजरने वाले सुरक्षित (HTTPS, आदि) ट्रैफिक सहित नेटवर्क पैकेटों को गहन स्कैन करने की क्षमता के साथ वेब गेटवे को सुरक्षित करने के लिए फोर्स पॉइंट एप्लिकेशन को लागू किया जाएगा।

14.2. उपयोगकर्ता एक्सेस प्रबंधन

14.2.1 उपयोगकर्ता पंजीकरण और विपंजीकरण

हडको के सभी आईटी सिस्टम तक एक्सेस प्रदान करने और रद्द करने के लिए एक औपचारिक प्रलेखित प्रक्रिया लागू की जाएगी।

सभी उपयोगकर्ता नाम विशिष्ट रूप से पहचान योग्य होने चाहिए तथा अस्वीकृत करने के सिद्धांतों का पालन किया जाना चाहिए।

स्वीकृत अनुरोध प्राप्त होने पर सुनिश्चित करें कि निर्दिष्ट समय-सीमा के भीतर उपयोगकर्ता आईडी को रद्द का काम पूरा हो जाए।

14.2.2 उपयोगकर्ता एक्सेस प्रावधान

सभी उपयोगकर्ता के एक्सेस अनुरोधों को उपयोगकर्ता के रिपोर्टिंग प्रबंधक द्वारा अधिकृत किया जाएगा। किसी उपयोगकर्ता को दी जाने वाली एक्सेस का स्तर, या उसे सौंपी जाने वाली भूमिका प्रोफ़ाइल, बिज़नस सिस्टम ओनर या उनके अनुमोदित प्रतिनिधियों/परियोजना प्रबंधक/रिपोर्टिंग प्रबंधकों द्वारा अनुमोदित की जाएगी।

यह अनुमोदक की जिम्मेदारी है कि वह समुचित जांच-पड़ताल के बाद यह सुनिश्चित करे कि व्यक्ति को अनुरोधित एक्सेस के स्तर के लिए वैध व्यावसायिक आवश्यकता है।

14.2.3 विशेषाधिकार एक्सेस अधिकारों का प्रबंधन

सूचना प्रणालियों पर विशेषाधिकार प्राप्त उपयोगकर्ता खातों/आईडी का निर्माण और आवंटन अधिकृत किया जाएगा। प्रक्रिया में निम्नलिखित सुनिश्चित किया जाएगा:

- प्रत्येक सिस्टम (जैसे ऑपरेटिंग सिस्टम, डेटाबेस और एप्लिकेशन) से जुड़े विशेषाधिकार और उनके संबंधित उपयोगकर्ताओं की पहचान की जाती है।
- विशेषाधिकार एक्सेस के लिए प्राधिकरण प्रक्रिया का कड़ाई से पालन करते हुए विशेषाधिकार व्यक्तियों को 'आवश्यकता' के आधार पर आवंटित किए जाते हैं ।
- सूचना प्रणाली पर उपयोग किए जाने वाले सभी विशेषाधिकार खातों का रिकॉर्ड रखना; विशेषाधिकार प्राप्त खातों में किए गए परिवर्तनों को रिकॉर्ड किया जाता है।

14.2.4 गुप्त प्रमाणीकरण जानकारी का प्रबंधन

- अस्थायी पासवर्ड केवल उपयोगकर्ता की पहचान की पुष्टि के बाद ही प्रदान किया जाएगा और यह उपयोगकर्ता को पहली बार उपयोग करने पर पासवर्ड बदलने के लिए संकेत देगा।
- या सॉफ़्टवेयर लगाने के बाद डिफ़ॉल्ट विक्रेता पासवर्ड में परिवर्तन करना आवश्यक है। ऐसे परिवर्तित पासवर्ड केवल विशेषाधिकार प्राप्त उपयोगकर्ताओं को ही आवश्यकता पड़ने पर ज्ञात होंगे।

14.2.5 उपयोगकर्ता एक्सेस अधिकारों की समीक्षा

महत्वपूर्ण या गोपनीय डेटा तक एक्सेस वाले खातों की, एक प्रलेखित व्यावसायिक प्रक्रिया का उपयोग करते हुए, अर्ध-वार्षिक समीक्षा की जाएगी। समीक्षा प्रक्रिया यह सत्यापित करेगी कि हडको छोड़ने वाले कर्मचारियों के पास अब सक्रिय खाते नहीं हैं, और भूमिकाएँ बदलने पर उन अनावश्यक अधिकारों को हटा दिया गया है, यह सुनिश्चित करने के लिए एक सतत प्रक्रिया लागू है।

14.2.6 एक्सेस अधिकारों को रद्द या समायोजित करना

सभी कार्मिकों और बाह्य पक्ष उपयोगकर्ताओं के सूचना और सूचना प्रसंस्करण सुविधाओं तक एक्सेस के अधिकार उनके रोजगार, अनुबंध या समझौते की समाप्ति पर हटा दिए जाएंगे, या परिवर्तन होने पर समायोजित कर दिए जाएंगे।

14.3. उपयोगकर्ता की ज़िम्मेदारियाँ

14.3.1 गुप्त प्रमाणीकरण जानकारी का उपयोग

यह आवश्यक है कि:

- पासवर्ड को लिखकर या स्पष्ट पृष्ठ में संग्रहीत नहीं किया जाना चाहिए।
- उपयोगकर्ता यह सुनिश्चित करेंगे कि पासवर्ड गोपनीय रखे जाएं तथा उन्हें आईटी हेल्प डेस्क सहित किसी के साथ साझा या प्रकट नहीं किया जाए।
- यदि उपयोगकर्ता को अस्थायी पासवर्ड प्रदान किया गया है, तो यह आवश्यक है कि अगली बार लॉगऑन करने पर उसे तुरन्त बदल दिया जाए।

14.4. सिस्टम और एप्लिकेशन एक्सेस नियंत्रण

14.4.1 सूचना एक्सेस प्रतिबंध

इस नीति और सहायक प्रक्रियाओं के अनुसार सूचना और अनुप्रयोग प्रणाली कार्यों तक एक्सेस प्रतिबंधित की जाएगी।

14.4.2 सुरक्षित लॉग-ऑन प्रक्रिया

सिस्टम और अनुप्रयोगों तक एक्सेस को सुरक्षित लॉग-ऑन प्रक्रिया द्वारा नियंत्रित किया जाएगा।

14.4.3 पासवर्ड प्रबंधन प्रणाली

उपयोगकर्ता पासवर्ड का आवंटन निम्नलिखित नियंत्रणों को लागू करके नियंत्रित किया जाएगा:

- उपयोगकर्ता आईडी यूनिक तथा खाते के लिए जिम्मेदार हडको ओनर तक पहुंच योग्य होगी।
- पासवर्ड की समाप्ति तिथि 90 दिन निर्धारित करें तथा पुनः उपयोग को रोकने के लिए कम से कम तीन पिछले पासवर्ड का इतिहास बनाए रखें।
- अल्फ़ान्यूमेरिक वर्णों सहित पासवर्ड की जटिलता लागू की जाएगी।
- पासवर्ड की लंबाई न्यूनतम आठ (8) अक्षरों की होनी चाहिए।
- पासवर्ड को ट्रांसमिशन और स्टोरेज में एन्क्रिप्ट या हैश किया जाएगा (अस्थायी पासवर्ड को छोड़कर)।

- अधिकतम पांच (5) असफल लॉगिन प्रयासों के बाद खाता लॉकआउट लागू किया जाएगा।
- सभी सामान्य उपयोगकर्ता खाते हडको के ओनर तक पहुंचने योग्य होंगे, जो खाते के लिए जिम्मेदार है। डिफ़ॉल्ट सॉफ़्टवेयर और हार्डवेयर खातों को या तो अक्षम करके या किसी विशिष्ट व्यक्ति तक पहुँचने योग्य ऑडिट ट्रेल बनाए रखकर प्रतिबंधित किया जाएगा।

14.4.4 डेटाबेस पासवर्ड प्रबंधन आवश्यकताएँ

- संगठन के आंतरिक डेटाबेस की सुरक्षा बनाए रखने के लिए, यह आवश्यक है कि सॉफ़्टवेयर प्रोग्रामों द्वारा एक्सेस केवल क्रेडेंशियल्स के साथ प्रमाणीकरण के बाद ही प्रदान की जाए। इस प्रमाणीकरण के लिए उपयोग किए जाने वाले क्रेडेंशियल्स को प्रोग्राम के स्रोत कोड के मुख्य, निष्पादन निकाय में स्पष्ट पृष्ठ में मौजूद होना आवश्यक नहीं है।
- डेटाबेस उपयोगकर्ता नाम और पासवर्ड प्रोग्राम के कोड के निष्पादन भाग से अलग एक फ़ाइल में संग्रहीत किए जाएँगे। यह फ़ाइल पठनीय नहीं होनी चाहिए।
- डेटाबेस क्रेडेंशियल्स डेटाबेस सर्वर पर स्थित हो सकते हैं। इस स्थिति में, क्रेडेंशियल्स की पहचान करने वाला एक हैश नंबर प्रोग्राम के कोड के निष्पादन निकाय में संग्रहीत किया जाएगा।
- डेटाबेस क्रेडेंशियल्स को एक प्रमाणीकरण सर्वर (अर्थात, एक एंटाइटेलमेंट निर्देशिका) के भाग के रूप में संग्रहीत किया जा सकता है, जैसे कि उपयोगकर्ता प्रमाणीकरण के लिए उपयोग किया जाने वाला LDAP सर्वर। डेटाबेस प्रमाणीकरण, प्रमाणीकरण सर्वर पर उपयोगकर्ता प्रमाणीकरण प्रक्रिया के भाग के रूप में, किसी प्रोग्राम की ओर से हो सकता है। इस स्थिति में, डेटाबेस क्रेडेंशियल्स के प्रोग्रामेटिक उपयोग की कोई आवश्यकता नहीं है।
- डेटाबेस एक्सेस के लिए उपयोग किए जाने वाले पासवर्ड या पास वाक्यांश पासवर्ड नीति का पालन करेंगे।
- किसी एकल व्यावसायिक कार्य को कार्यान्वित करने वाले प्रत्येक प्रोग्राम या प्रोग्रामों के प्रत्येक संग्रह के लिए विशिष्ट डेटाबेस क्रेडेंशियल्स होने चाहिए। प्रोग्रामों के बीच क्रेडेंशियल्स को साझा करने की अनुमति नहीं है।
- प्रोग्रामों द्वारा उपयोग किए जाने वाले डेटाबेस पासवर्ड, पासवर्ड दिशानिर्देशों द्वारा परिभाषित सिस्टम-स्तरीय पासवर्ड होंगे।
- डेवलपर समूहों के पास यह सुनिश्चित करने के लिए एक प्रक्रिया होगी कि डेटाबेस पासवर्ड को पासवर्ड दिशानिर्देशों के अनुसार नियंत्रित और परिवर्तित किया जाए।
- इस प्रक्रिया में डेटाबेस पासवर्ड के ज्ञान को आवश्यकता के आधार पर सीमित करने की विधि शामिल होगी।

14.4.5 विशेषाधिकार उपयोगिता कार्यक्रम का उपयोग

- ऐसे महत्वपूर्ण उपयोगिता कार्यक्रम, जो सिस्टम और अनुप्रयोग नियंत्रणों को ओवरराइड करने में सक्षम हो सकते हैं, प्रतिबंधित और कड़े नियंत्रण में रखा जाएगा।
- ब्राउज़र में LAN सेटिंग विकल्पों सहित सभी अनावश्यक उपयोगिता प्रोग्राम हटा दिए जाएंगे या अक्षम कर दिए जाएंगे।

14.4.6 प्रोग्राम स्रोत कोड तक एक्सेस नियंत्रण

- कार्यक्रम स्रोत कोड तक एक्सेस प्रतिबंधित होगी और उसका उचित दस्तावेजीकरण किया जाएगा।
- प्रोग्राम स्रोत कोड और प्रोग्राम स्रोत लाइब्रेरीज़ को स्थापित प्रक्रियाओं के अनुसार प्रबंधित किया जाएगा।

15. ऑडिट लॉग का रखरखाव, निगरानी और विश्लेषण

सुरक्षा घटनाओं का पता लगाने के लिए लॉगिंग, निगरानी और रिपोर्टिंग क्षमताओं को क्रियान्वित किया जाएगा।

- लॉग जनरेशन-हडको लॉग स्रोत की पहचान करेगा, लॉग उत्पन्न करने वाले सभी सिस्टम, एप्लिकेशन और डिवाइस का निर्धारण करेगा।
- लॉग सामग्री: सुनिश्चित करें कि लॉग में प्रासंगिक जानकारी जैसे टाइमस्टैम्प, ईवेंट प्रकार, उपयोगकर्ता गतिविधियाँ, स्रोत और गंतव्य आईपी, पते आदि शामिल हों।
- लॉग प्रारूप: आसान विश्लेषण की सुविधा के लिए विभिन्न स्रोतों में लॉग प्रारूपों को मानकीकृत करें।
- केंद्रीकृत लॉग संग्रहण: हडको विभिन्न स्रोतों से लॉग को एक केंद्रीकृत लॉग प्रबंधन प्रणाली या सुरक्षा सूचना और घटना प्रबंधन (एसआईईएम) प्रणाली में एकत्रित करेगा।
- सुरक्षित ट्रांसमिशन: हुडको यह सुनिश्चित करेगा कि लॉग्स को एन्क्रिप्शन का उपयोग करके सुरक्षित रूप से प्रेषित किया जाए ताकि अवरोधन और छेड़छाड़ से बचा जा सके।
- प्रतिधारण नीति: हडको एक लॉग प्रतिधारण नीति को परिभाषित और कार्यान्वित करेगा, जिसमें आमतौर पर कम से कम छह महीने के लिए या नियामक आवश्यकताओं के अनुसार लॉग को बनाए रखा जाएगा।
- रखरखाव सुरक्षा: अनधिकृत एक्सेस, संशोधन या विलोपन को रोकने के लिए लॉग को एक्सेस नियंत्रण के साथ सुरक्षित वातावरण में संग्रहीत करें।
- अतिरेक: हडको यह सुनिश्चित करेगा कि डेटा हानि से बचाने के लिए लॉग्स को अतिरेक रूप से संग्रहीत किया जाए।
- वास्तविक समय निगरानी: हडको संदिग्ध गतिविधियों और सुरक्षा चक्र का तुरंत पता लगाने के लिए लॉग की वास्तविक समय निगरानी लागू करेगा।
- स्वचालित विश्लेषण: हडको पैटर्न, विसंगतियों और समझौता के ज्ञात संकेतकों (आईओसी) के लिए लॉग का विश्लेषण करने के लिए स्वचालित उपकरणों और स्क्रिप्ट का उपयोग करेगा।
- मैनुअल समीक्षा: हडको किसी भी छूटी हुई विसंगति या घटना की पहचान करने के लिए लॉग की नियमित मैनुअल समीक्षा करेगा।
- लॉग को गंभीरता और जोखिम मूल्यांकन के आधार पर हडको के केंद्रीकृत सुरक्षा परिचालन केंद्र (एसओसी) के साथ एकीकृत किया जाना चाहिए।
- हडको एक व्यवस्थित तरीके से ऑडिट लॉग का प्रबंधन और विश्लेषण करने के लिए एक केंद्रीकृत एप्लिकेशन का उपयोग करेगा ताकि किसी हमले का पता लगाया जा सके, उसे समझा जा सके या उससे उबरा जा सके।

16. ऑडिट ट्रेल्स

प्रत्येक आईटी एप्लिकेशन, जो महत्वपूर्ण या संवेदनशील जानकारी तक पहुँच सकता है या उस पर प्रभाव डाल सकता है, में आवश्यक ऑडिट और सिस्टम लॉगिंग क्षमताएँ शामिल होनी चाहिए, जिससे व्यापक ऑडिट ट्रेल्स का प्रावधान सुनिश्चित हो सके। ये ऑडिट ट्रेल्स नियामक और कानूनी आदेशों के अलावा हडको की व्यावसायिक आवश्यकताओं को भी पूरा करने चाहिए।

ऑडिट ट्रेल्स में पर्याप्त विवरण होना चाहिए ताकि वे ऑडिट प्रक्रियाओं का समर्थन कर सकें, आवश्यकता पड़ने पर फोरेंसिक साक्ष्य के रूप में काम कर सकें, और विवाद समाधान में सहायता कर सकें, जिसमें गैर-अस्वीकृति सुनिश्चित करना भी शामिल है। हडको किसी भी अनधिकृत गतिविधि की पहचान करने और उसका समाधान करने के लिए ऑडिट ट्रेल्स और सिस्टम लॉग्स की नियमित निगरानी हेतु एक प्रणाली स्थापित करेगा।

17. क्रिप्टोग्राफी

17.1 क्रिप्टोग्राफी नियंत्रण

17.1.1 क्रिप्टोग्राफ़िक नियंत्रणों के उपयोग पर नीति

- ट्रांसमिशन चैनलों, डेटा प्रोसेसिंग और प्रमाणीकरण उद्देश्यों में प्रयुक्त कुंजी लंबाई, एल्गोरिदम, सिफर सूट और लागू प्रोटोकॉल मज़बूत होने चाहिए। हडको अंतरराष्ट्रीय स्तर पर स्वीकृत और प्रकाशित मानकों को अपनाएँगे जो अप्रचलित/असुरक्षित/भेद्य न हों और ऐसे नियंत्रणों को लागू करने में शामिल विन्यास मौजूदा कानूनों और नियामक निर्देशों के अनुरूप होने चाहिए।
- हडको, पारगमन या संग्रहीत सूचना के महत्व को समझता है इसलिए, जहाँ भी संभव और उपयुक्त हो, क्रिप्टोग्राफ़िक कुंजियों और प्रमाणपत्र प्रबंधन के माध्यम से इसे सुरक्षित रखने का प्रयास करता है। सुरक्षा का स्तर सूचना की संवेदनशीलता और उपयोग की आवृत्ति के साथ-साथ उस वातावरण के अनुरूप होना चाहिए जहाँ वह रहती/उपयोग की जाती है।
- कुंजी संरक्षकों को अवगत करावाया जाएगा, और उन्हें कुंजियों की सुरक्षा के प्रबंधन में अपने दायित्वों को औपचारिक रूप से स्वीकार करना होगा।

17.2 कुंजी प्रबंधन

कुंजी निर्माण, स्वामित्व, वितरण, अभिलेखीकरण, रखरखाव और निरसन के लिए यह आवश्यक है कि एन्क्रिप्शन कुंजी प्रबंधन दिशानिर्देशों को परिभाषित, जारी और पालन किया जाए ताकि कुंजियों की संपूर्ण जीवन-चक्र में सुरक्षा सुनिश्चित की जा सके। प्रक्रिया दस्तावेज़ों में कुंजी प्रबंधन से संबंधित निम्नलिखित पहलुओं पर ध्यान दिया जाएगा, जिनमें शामिल हैं:

- कुंजी निर्माण;
- कुंजी वितरण;
- कुंजी रख रखाव;
- कुंजी परिवर्तन;
- कुंजी विनाश;
- दोहरे नियंत्रण के लिए प्रमुख संरक्षक और आवश्यकताएं;
- कुंजियों के अनधिकृत प्रतिस्थापन की रोकथाम;
- ज्ञात या संदिग्ध समझौता की कुंजियों का प्रतिस्थापन;
- निर्धारित क्रिप्टो अवधि के अंत में क्रिप्टोग्राफिक कुंजी में परिवर्तन।

यह आवश्यक है कि क्रिप्टोग्राफिक कुंजियों को अनधिकृत संशोधन, प्रतिस्थापन, अनपेक्षित विनाश और हानि से सुरक्षित रखा जाए।

सममित क्रिप्टोग्राफिक एल्गोरिदम से जुड़ी गुप्त कुंजियों और असममित क्रिप्टो प्रणालियों से जुड़ी निजी कुंजियों को अनधिकृत प्रकटीकरण से सुरक्षित रखा जाएगा।

18 मेकर चैकर

- सूचना प्रणाली में सभी हडको कार्मिकों के लिए मेकर चेकर सिद्धांत लागू किया जाएगा।
- हडको एक उपयुक्त निर्माता जांच प्रणाली स्थापित करेगा ताकि यह सुनिश्चित किया जा सके कि संबंधित प्रस्तुतीकरण सही और त्रुटि रहित है।

19 भेद्यता प्रबंधन

- उपयोग की जा रही सूचना प्रणालियों की तकनीकी कमज़ोरियों के बारे में आंतरिक टीमों, बाहरी टीमों और स्रोतों द्वारा समय पर जानकारी प्राप्त की जाएगी। हडको की ऐसी कमज़ोरियों के प्रति संवेदनशीलता का मूल्यांकन किया जाएगा और संबंधित जोखिम को दूर करने के लिए उचित उपाय किए जाएँगे।
- भेद्यता आकलन (वीए) / प्रवेश परीक्षण (पीटी) का संचालन (क) महत्वपूर्ण सूचना प्रणालियों और/या ग्राहक संपर्क वाले असैन्यीकृत क्षेत्र (डीएमजेड) में स्थित प्रणालियों हेतु, वीए हर छह महीने में कम से कम एक बार और पीटी हर 12 महीने में कम से कम एक बार किया जाएगा। इसके अतरिक्त, हडको ऐसी सूचना प्रणालियों के पूरे जीवनचक्र (कार्यान्वयन से पहले, कार्यान्वयन के बाद, बड़े बदलावों के बाद, आदि) के दौरान वीए/पीटी का संचालन करेगा।
- हडको वीए/पीटी के संचालन हेतु एक प्रलेखित दृष्टिकोण अपनाएगा जिसमें दायरा, कवरेज, भेद्यता स्कोरिंग प्रणाली (जैसे, कॉमन वल्नरेबिलिटी स्कोरिंग सिस्टम) और अन्य सभी पहलुओं को शामिल किया जाएगा। यह क्लाउड वातावरण में होस्ट की गई हडको की सूचना प्रणालियों पर भी लागू हो सकता है।
- इंटरनेट से जुड़े वेब/मोबाइल/क्लाउड-आधारित अनुप्रयोगों, सर्वरों और नेटवर्क घटकों का उनके पूरे जीवनचक्र में वीए/पीटी (VA/PT) करना। ऐसा मूल्यांकन केवल प्रोफेशनल रूप से योग्य टीमों द्वारा ही किया जाएगा।
- यह सुनिश्चित करना कि भेद्यता स्कैनिंग उपकरण अपनाए/कार्यान्वित किए जाएं तथा उन्हें नवीनतम सुरक्षा भेद्यता जानकारी के साथ नियमित रूप से अद्यतन किया जाए।
- सूचना सुरक्षा टीम द्वारा हडको सिस्टम, नेटवर्कों और डेटा के जोखिम के अनुरूप सुधार के लिए कमजोरियों और सिस्टम पैच को प्राथमिकता दी जाएगी।
- सिस्टम, एप्लिकेशन, सर्वर और नेटवर्क डिवाइस के लिए भेद्यता निवारण और पैचिंग गतिविधि को निर्धारित समयसीमा के अनुसार ट्रैक किया जाएगा।
- परीक्षण वातावरण में महत्वपूर्ण पैचों का मूल्यांकन उत्पादन सिस्टम पर डालने से पहले किया जाएगा।
- ईआरपी सिस्टम, आईसीटी बुनियादी ढांचे सहित पहचानी गई कमजोरियों के समाधान में तेजी लाना।
- सुरक्षा जोखिम बढ़ाने वाली वेबसाइटों और सभी गैर-व्यावसायिक वेबसाइटों की गहन समीक्षा करें और उन्हें ब्लॉक करें।

20 साइबर सुरक्षा तैयारी संकेतक

- सूचना और साइबर जोखिम तैयारी के स्तर का आकलन हेतु सूचना सुरक्षा समिति द्वारा नियमित अंतराल पर मैन्युअल रूप से या स्वचालित उपकरणों की सहायता से तकनीकी अनुपालन जांच की जाएगी।
- सभी कार्यों को उत्पादन वातावरण में तैनाती से पहले सीआईएसओ कार्यालय से सूचना सुरक्षा प्रभाव वाली परियोजनाओं, उत्पादों, अनुप्रयोगों, सेवाओं आदि के लिए सुरक्षा मंजूरी प्राप्त करनी चाहिए।
- तकनीकी अनुपालन जांच में प्रवेश परीक्षण, भेद्यता आकलन, वास्तुकला समीक्षा शामिल होगी जो आंतरिक रूप से या इस उद्देश्य के लिए विशेष रूप से अनुबंधित स्वतंत्र विशेषज्ञों द्वारा की जा सकती है।
- सीआईएसओ तिमाही आधार पर आईटी कौशलनीति समिति को सूचना सुरक्षा तैयारी और व्यवस्था की रिपोर्ट देगा।

20.1 साइबर संकट प्रबंधन कौशलनीति

साइबर घटना से निपटने की गतिविधियों में शामिल हैं:

- घटना का पता लगाना
- घटना की रिपोर्टिंग
- समाधान में प्रतिक्रिया, नियंत्रण और समाधान शामिल हैं।
- रिकवरी यह पहचानती है कि प्रभावित सिस्टम को सुरक्षित रूप से पुनः उत्पादन में कैसे लाया जाए।
- घटना का सफलतापूर्वक समाधान सुनिश्चित करने के लिए और इसके समाधान से सूचना परिसंपत्ति पर कोई सुरक्षा प्रभाव नहीं पड़ा है, समाधान के बाद समीक्षा की जाती है।
- मूल कारण विश्लेषण से यह पता चलता है कि कोई घटना क्यों घटित हुई, तथा मूल कारण को समाप्त करने के लिए सुधारात्मक कार्य योजना तैयार की जाती है।

20.2 साइबर हमलों का सामना करने के लिए तैयारी का परीक्षण करें

20.2.1 अभ्यास और परीक्षण

सीआईएसओ के साथ समन्वय में आईटी विभाग, संकट सिमुलेशन अभ्यास, मॉक ड्रिल, रेड टीमिंग अभ्यास आदि जैसे विभिन्न अभ्यास विकसित करेगा, जो साइबर संकट प्रबंधन योजना की पर्याप्तता और निरंतरता का आकलन करेंगे। हडको की रक्षात्मक और प्रतिक्रियात्मक क्षमताओं को मापने के लिए परीक्षण अभ्यास भी किए जाएँगे। ये अभ्यास परीक्षण नियोजित अंतरालों पर या जब भी महत्वपूर्ण परिवर्तन होते हैं, आयोजित किए जाएँगे। लचीलापन परीक्षण साइबर संकट प्रबंधन योजना (सीसीएमपी) के दायरे और उसके उद्देश्यों के अनुरूप आयोजित किए जाने हैं। लचीलापन परीक्षण उपयुक्त परिदृश्यों पर आधारित होने चाहिए, जो सुनियोजित हों और जिनके लक्ष्य और उद्देश्य स्पष्ट रूप से परिभाषित हों। अभ्यास के बाद की रिपोर्ट में परिणामों की सिफ़ारिशें और सुधार को लागू करने के लिए कार्रवाई शामिल होनी चाहिए।

20.2.2 साइबर घटना पर हडको प्रतिक्रिया और पुनर्प्राप्ति प्रबंधन

- साइबर घटना प्रतिक्रिया और पुनर्प्राप्ति प्रबंधन नीति में घटनाओं के वर्गीकरण और मूल्यांकन को संबोधित किया जाएगा; इसमें ऐसी घटनाओं के प्रबंधन, जोखिम को नियंत्रित करने और समय पर पुनर्प्राप्ति प्राप्त करने के लिए एक स्पष्ट संचार कौशलनीति और योजना शामिल होगी।

- हडको साइबर घटनाओं का विश्लेषण करेगा (यदि आवश्यक हो तो फोरेंसिक विश्लेषण सहित) ताकि उनकी गंभीरता, प्रभाव और मूल कारण का पता लगाया जा सके। हडको व्यावसायिक संचालन पर घटनाओं के प्रतिकूल प्रभाव को कम करने के लिए सुधारात्मक और निवारक उपाय करेगा।
- हडको के पास घटना प्रतिक्रिया और पुनर्प्राप्ति प्रक्रिया लिखित होगी, जिसमें ऐसी घटनाओं से निपटने वाले कार्मिकों/आउटसोर्स कार्मिकों की प्रमुख भूमिकाओं की पहचान शामिल होगी।
- बोर्ड और वरिष्ठ प्रबंधन के साथ-साथ ग्राहकों को घटनाओं की सूचना देने और उन्हें आगे बढ़ाने के लिए हडको के पास, आवश्यकतानुसार स्पष्ट संचार योजनाएँ होंगी। नियामक आवश्यकताओं के अनुसार, घटनाओं के संबंध में CERT-In और आरबीआई को हडको सक्रिय रूप से सूचित करेगा।
- पिछली घटनाओं से सीख लेकर, साथ ही परीक्षणों और अभ्यासों के माध्यम से, घटना प्रतिक्रिया और पुनर्प्राप्ति गतिविधियों और क्षमताओं में सुधार के लिए हडको प्रक्रियाएँ स्थापित करेगा। इसके अतिरिक्त हितधारकों (सेवा प्रदाताओं सहित) के साथ हडको आवधिक अभ्यास/परीक्षण आयोजित करके संकट संचार योजना/प्रक्रिया की प्रभावशीलता सुनिश्चित करेगा।

20.2.3 व्यवसाय निरंतरता प्रबंधन

साइबर सुरक्षा को संगठन की व्यावसायिक निरंतरता प्रबंधन सिस्टम में अंतर्निहित किया जाएगा। आपदाओं की स्थिति में संचालन की निरंतरता सुनिश्चित करने के लिए व्यावसायिक निरंतरता योजना और प्रक्रियाओं की स्थापना और रखरखाव किया जाएगा।

- हडको व्यवसाय निरंतरता प्रबंधन को समर्थन देने के लिए एक आईटी प्रक्रिया स्थापित और कार्यान्वित करेगा, ताकि यह सुनिश्चित किया जा सके कि किसी प्राकृतिक या मानव निर्मित आपदा की स्थिति में, व्यवसाय-महत्वपूर्ण सूचना प्रसंस्करण सेवाएं और प्रणालियां निर्धारित समय सीमा के भीतर बहाल हो जाएं। प्रणालियों को निर्धारित समय सीमा के भीतर बहाल किया जाता है।
- आईटी विभाग इस प्रक्रिया का ओनर होगा। यह प्रक्रिया व्यावसायिक प्रक्रियाओं पर आपदाओं के जोखिम मूल्यांकन और प्रभाव को समझेगी और आपदा पुनर्प्राप्ति तथा आईटी आकस्मिकता योजनाओं के विकास को आगे बढ़ाएगी, जिनका समर्थन उनके निरंतर रखरखाव (सुधार) द्वारा किया जाएगा।
- हडको महत्वपूर्ण व्यावसायिक प्रक्रियाओं की पहचान करेगा और निरंतरता योजनाओं की आवश्यकताओं को निर्धारित करने के लिए आपदाओं के कारण होने वाले व्यवधानों के कारण औपचारिक जोखिम मूल्यांकन और व्यावसायिक प्रभाव विश्लेषण करेगा।
- व्यवसाय निरंतरता और प्रभाव विश्लेषण द्वारा पहचानी गई आवश्यकताओं के आधार पर व्यवसाय निरंतरता योजनाएं विकसित की जाएंगी।
- हडको निरंतरता योजनाओं के आवधिक परीक्षण के लिए एक कार्यक्रम निर्धारित करेगा। परीक्षण यह सत्यापित करने के लिए किया जाएगा कि योजनाएँ व्यावहारिक हैं और कार्मिकों को योजनाओं के संचालन से परिचित करवाने के लिए प्रशिक्षण दिया जाएगा।
- व्यवसाय निरंतरता योजनाओं की समीक्षा की जाएगी और उन्हें वर्ष में कम से कम एक बार अद्यतन किया जाएगा।
- हडको सभी महत्वपूर्ण बैकअप का एक सेट (प्रतिलिपि) ऑफ़साइट, यानी अपने परिसर से दूर संग्रहीत करेगा। बैकअप रखने की ऑफ़साइट व्यवस्था, बैकअप में संग्रहीत जानकारी के वर्गीकरण के अनुसार होगी।

21 घटना रिपोर्टिंग

- सभी सूचना और साइबर सुरक्षा घटनाओं की सूचना, सूचना सुरक्षा समिति को दी जाएगी।
- हडको की आईटी प्रणालियों से समझौता करने वाली घटनाएं जैसे डेटा का उल्लंघन, डेटा का विनाश आदि, जो कंपनी के संचालन को गंभीर रूप से प्रभावित करती हैं, हडको द्वारा उन पर की गई कार्रवाई के साथ आवश्यकतानुसार सीईआरटी-इन/अन्य वैधानिक निकायों को सूचित की जाएंगी।
- सभी सूचनाएं और साइबर सुरक्षा घटनाएं साइबर सुरक्षा घटना डेटाबेस में दर्ज की जाएंगी।
- घुसपैठ, हमलों और धोखाधड़ी की सक्रिय निगरानी के लिए निगरानी सुविधा स्थापित की जाएगी।
- उपयोगकर्ता समुदाय को सूचना और साइबर सुरक्षा घटनाओं की पहचान करने और रिपोर्ट करने के तरीके के बारे में शिक्षित किया जाएगा।
- बड़ी और गंभीर रूप में वर्गीकृत घटनाओं की सूचना सीआईएसओ, प्रमुख (आईटी) और अन्य संबंधित शेयरधारकों को दी जानी चाहिए।

22 डिजिटल हस्ताक्षर

डिजिटल हस्ताक्षरों को सूचना प्रौद्योगिकी अधिनियम 2000 द्वारा प्रस्तुत किया गया था और 2008 में इसके संशोधन में इसे और विस्तृत किया गया। इस अधिनियम में प्रमाणन प्राधिकरण नियंत्रक (सीसीए) के गठन का प्रावधान किया गया, जिसने प्रमाणन प्राधिकरण (सीए) का गठन किया, जिसने देश के लिए सार्वजनिक कुंजी अवसंरचना (पीकेआई) का निर्माण किया।

डिजिटल हस्ताक्षर का उपयोग संदेश भेजने वाले या दस्तावेज़ पर हस्ताक्षर करने वाले की पहचान प्रमाणित करने हेतु और यह सुनिश्चित करने के लिए किया जाता है कि भेजे गए संदेश या दस्तावेज़ की मूल सामग्री अपरिवर्तित है।

डिजिटल हस्ताक्षर निम्नलिखित तीन विशेषताएं प्रदान करते हैं:

प्रमाणीकरण- डिजिटल हस्ताक्षरों का उपयोग संदेशों के स्रोत को प्रमाणित करने के लिए किया जाता है। डिजिटल हस्ताक्षर कुंजी का ओनर एक विशिष्ट उपयोगकर्ता के पास होता है। इस प्रकार एक वैध हस्ताक्षर यह दर्शाता है कि संदेश उसी उपयोगकर्ता द्वारा भेजा गया था।

अखंडता - कई परिस्थितियों में, संदेश भेजने वाले और प्राप्त करने वाले को यह आश्वासन चाहिए होता है कि संदेश प्रेषण के दौरान उसमें कोई बदलाव नहीं किया गया है। डिजिटल हस्ताक्षर क्रिप्टोग्राफ़िक संदेश डाइजेस्ट फ़ंक्शन का उपयोग करके यह सुविधा प्रदान करते हैं।

अस्वीकरण - डिजिटल हस्ताक्षर यह सुनिश्चित करते हैं कि सूचना पर हस्ताक्षर करने वाला प्रेषक बाद में हस्ताक्षर करने से इनकार नहीं कर सकेगा।

23 सोशल मीडिया जोखिम

सोशल मीडिया दिशानिर्देशों का उद्देश्य अधिकृत कार्मिकों को विभिन्न व्यावसायिक उद्देश्यों के लिए सोशल मीडिया के सुरक्षित उपयोग के लिए मार्गदर्शन प्रदान करना है।

हडको नीचे दिए गए सोशल मीडिया दिशानिर्देशों का पालन करता है:

- केवल अधिकृत उपयोगकर्ता/विक्रेता ही सोशल मीडिया अकाउंट का प्रबंधन करेंगे।
- सोशल मीडिया गतिविधियों के लिए केवल आधिकारिक हडको सोशल मीडिया अकाउंट का ही उपयोग किया जाएगा।
- हडको द्वारा केवल सुरक्षित (https://) सोशल मीडिया प्लेटफॉर्म का ही उपयोग किया जाएगा।
- सोशल मीडिया अकाउंट हुडको द्वारा जारी डेस्कटॉप/लैपटॉप या अधिकृत तृतीय पक्ष विक्रेता के सिस्टम से संचालित किए जाएँगे।
- केवल अधिकृत कार्मिकों को ही सोशल मीडिया पर कोई आधिकारिक टिप्पणी पोस्ट करने की अनुमति दी जानी चाहिए।
- कार्मिकों/विक्रेताओं को ऐसी कोई भी जानकारी प्रकाशित, पोस्ट या जारी नहीं करनी चाहिए जो गोपनीय मानी जाती हो या सार्वजनिक न की गई हो। अगर किसी जानकारी को गोपनीय माना जाता है, तो कार्मिकों को अपने पर्यवेक्षक से इसकी जाँच कर लेनी चाहिए।
- कार्मिकों को किसी तीसरे पक्ष के कॉपीराइट, कॉपीराइट सामग्री, ट्रेडमार्क, सेवा चिह्न या अन्य बौद्धिक संपदा का उपयोग करने के लिए उचित अनुमति लेनी होगी।
- हालांकि यह कोई विशिष्ट सूची नहीं है, लेकिन निषिद्ध सोशल मीडिया सामग्री के कुछ विशिष्ट उदाहरणों में ऐसी टिप्पणियां, सामग्री या चित्र पोस्ट करना शामिल है जो अपमानजनक, अश्लील, स्वामित्वपूर्ण, उत्पीड़नकारी हों या जो शत्रुतापूर्ण कार्य वातावरण बना सकते हों।

24 भौतिक और पर्यावरणीय सुरक्षा

इस नीति का उद्देश्य सूचना परिसंपत्तियों के साथ-साथ सहायक सेवाओं और प्रक्रियाओं को भौतिक और पर्यावरणीय खतरों से बचाना है। भौतिक खतरों में भौतिक छेड़छाड़, अनधिकृत निष्कासन, क्षति और चोरी शामिल हैं। पर्यावरणीय खतरों में भूकंप, बाढ़, आग, नागरिक अशांति और अन्य प्राकृतिक एवं मानव निर्मित आपदाएँ शामिल हैं।

24.1 सुरक्षित क्षेत्र

24.1.1 भौतिक सुरक्षा परिधि

- यह आवश्यक है कि परिसर और सुरक्षित क्षेत्रों तक उचित एक्सेस बनाए रखी जाए ताकि अनधिकृत व्यक्तियों को व्यक्तिगत पहुंच से रोका जा सके।
- सुरक्षित क्षेत्रों तक एक्सेस केवल उन आगंतुकों को दी जाती है जिनके पास सुरक्षित क्षेत्र में जाने का वास्तविक पहचान योग्य कारण हो।
- परिसर में प्रवेश देने से पहले व्यक्तियों को पहचान पत्र जारी किया जाना यह आवश्यक है।
- भवन में व्यक्तिगत पहुँच को नियंत्रित करने के लिए एक मानवयुक्त स्वागत क्षेत्र या अन्य साधन मौजूद होने चाहिए। यह आवश्यक है कि सुरक्षित क्षेत्रों तक पहुँच केवल अधिकृत कर्मियों तक ही सीमित हो।
- यह सुनिश्चित किया जाएगा कि सुरक्षित क्षेत्रों तक पहुंच के अधिकारों की नियमित रूप से समीक्षा की जाए और उन्हें अद्यतन किया जाए।
- यह आवश्यक है कि दूरस्थ स्थान जहां डेटा संसाधित या संग्रहीत किया जाता है, वहां एक्सेस नियंत्रण और सुरक्षा प्रदान की जाए जिससे हानि या क्षति का जोखिम स्तर तक कम हो जाए।
- स्थान(स्थानों) और/या मंजिल(मंजिलों) के बीच सूचना परिसंपत्तियों की सभी गतिविधियों को अधिकृत कर्मियों द्वारा नियंत्रित किया जाना है।

- यह सुनिश्चित किया जाएगा कि डिलीवरी और लोडिंग क्षेत्रों जैसे प्रवेश द्वार और अन्य द्वार, जहां अनधिकृत व्यक्ति परिसर में प्रवेश कर सकते हैं, को अनधिकृत एक्सेस से बचने के लिए नियंत्रित किया जाना चाहिए।
- हडको डेटा सेंटर (डीसी) में व्यक्तिगत सुरक्षा नियंत्रण होना आवश्यक है जो अनधिकृत व्यक्तियों को व्यक्तिगत पहुँच करने से रोकता है। इन नियंत्रणों में निम्नलिखित शामिल होना आवश्यक है:
    - डेटा सेंटर के सभी प्रवेश द्वार पर प्रवेश और निकास दोनों के लिए अभिगम नियंत्रण सुविधा उपलब्ध है। बायोमेट्रिक्स या एक्सेस कार्ड जैसे प्रौद्योगिकी-आधारित अभिगम नियंत्रण समाधान उपलब्ध होना आवश्यक है।
    - डेटा सेंटर तक व्यक्तिगत पहुंच प्रतिबंधित होगी।
    - सर्वर, डिस्क, टेप और अन्य नेटवर्क उपकरण रखने वाली अलमारियाँ बंद दरवाजों से सुरक्षित हैं। सर्वर रूम में सभी रैक को लॉक किया जाना चाहिए। इन रैकों तक पहुंच केवल अधिकृत कर्मियों तक ही सीमित होगी।
    - डेटा सेंटर तक पहुंच केवल व्यावसायिक आवश्यकता और आईटी प्रमुख से अनुमोदन के बाद ही दी जाएगी।
    - डेटा सेंटर तक एक्सेस को अनुमोदित और लॉग किया जाना है।
    - सभी क्षेत्रों के लिए एक्सेस लॉग को न्यूनतम छह (6) महीने की अवधि के लिए बनाए रखा जाना आवश्यक है।
    - सर्वर रूम तक एक्सेस लॉग की समीक्षा की जाएगी ताकि यह सुनिश्चित किया जा सके कि केवल उचित एक्सेस ही दी जाए।
    - फोटो पहचान पत्र के साथ प्रवेश नियंत्रण कार्ड उन उपयोगकर्ताओं को प्रदान किए जा सकते हैं जिन्हें आवश्यकता के आधार पर सर्वर रूम तक जाने की आवश्यकता होती है।
    - आगंतुक कार्ड गैर-कर्मचारियों अर्थात विक्रेताओं, लेखा परीक्षकों, आगंतुकों को जारी किए जा सकते हैं।
    - सर्वर रूम के सभी प्रवेश द्वारों और सर्वर रूम के भीतर की गतिविधियों पर क्लोज्ड सर्किट टेलीविजन (सीसीटीवी) द्वारा निगरानी रखी जाएगी। यह आवश्यक है कि कोई भी व्यक्तिगत पहुंच/प्रवेश द्वार निगरानी से मुक्त न रहे।
    - लोगों और परिसंपत्तियों की आवाजाही पर नजर रखने और सुविधा प्रभारी से पूर्व अनुमति लेकर हार्ड परिसंपत्तियों की सूची एकत्र करने के प्रयोजनों के अलावा सर्वर रूम में फोटोग्राफी और वीडियो शूटिंग प्रतिबंधित है।
    - यह सुनिश्चित किया जाएगा कि सुरक्षा गार्ड यह सुनिश्चित करें कि सर्वर रूम के अंदर या बाहर आईटी उपकरणों की कोई अनधिकृत आवाजाही न हो।
    - यह सुनिश्चित किया जाएगा कि परिसर में प्रवेश करने वाले सभी कार्मिक यह घोषित करें कि क्या वे कोई आईटी उपकरण जैसे स्टोरेज मीडिया या पोर्टेबल स्टोरेज डिवाइस ले जा रहे हैं।

सर्वर रूम से जानकारी के नुकसान को रोकने के लिए पोर्टेबल स्टोरेज डिवाइस ले जाना सख्त वर्जित है। यदि सर्वर रूम से कोई वस्तु बाहर ले जानी हो, तो अधिकृत कर्मियों द्वारा उपयुक्त गेट पास जारी करना और सुविधा प्रभारी/परियोजना प्रभारी से पूर्व अनुमति लेकर हार्ड एसेट्स की सूची एकत्र करना आवश्यक है।

24.1.2 व्यक्तिगत प्रवेश

- सभी आगंतुकों को रिसेप्शन पर आगंतुक रजिस्टर में प्रविष्टि करनी होगी, जिसके बाद एक अस्थायी आईडी कार्ड/आगंतुक कार्ड जारी किया जाएगा जिसे हडको परिसर में हर समय उसे पहने हुए दिखाई देना चाहिए।
- यह सुनिश्चित किया जाएगा कि आगंतुकों को उनके गंतव्य तक लाने और ले जाने के लिए एस्कॉर्ट या हडको का संबंधित अधिकारी मौजूद हो।
- लैपटॉप, पेन ड्राइव और अन्य रिमूवेबल स्टोरेज मीडिया को डेटा सेंटर प्रशासक की पूर्व स्वीकृति के बिना डेटा सेंटर में प्रवेश की अनुमति नहीं है।
- आगंतुकों की मेजबानी करने वाले कार्मिक के लिए यह आवश्यक है कि:
    - विजित से पूर्व साइट सुरक्षा को सूचना दें; आगंतुक द्वारा प्रतिनिधित्व किए जाने वाले नाम और कंपनी का उल्लेख करें।
    - रिसेप्शन (या साइट सुरक्षा डेस्क) से आगंतुक(ओं) को ले जाना/वापस करना।
    - हडको परिसर में हर समय आगंतुक को अनुरक्षित रखें।
- परिचालन क्षेत्र जैसे सुरक्षित क्षेत्रों में आने वाले आगंतुकों की निगरानी की जानी चाहिए तथा उनके प्रवेश और प्रस्थान की तारीख और समय दर्ज किया जाना चाहिए।
- यह आवश्यक है कि सभी कर्मचारी कंपनी परिसर में हर समय अपना पहचान पत्र प्रदर्शित करें।
- सभी कर्मचारियों, संविदा कर्मचारियों और विक्रेता कर्मचारियों को जारी किए गए एक्सेस कार्ड का उपयोग भवन के भीतर नियंत्रण क्षेत्रों तक पहुँच प्राप्त करने के लिए किया जाना है। यह एक्सेस कार्ड प्रत्येक व्यक्ति का निजी होता है, इसलिए यह आवश्यक है कि इसे अन्य कर्मचारियों के साथ साझा न किया जाए।
- नौकरी छोड़ने वाले कर्मचारियों के प्रवेश अधिकार तुरंत रद्द कर दिए जाएंगे।

24.1.3 कार्यालयों, कमरों और सुविधाओं की सुरक्षा

- प्रमुख सुविधाओं को जनता की पहुंच से दूर रखा जाएगा।
- यह सुनिश्चित किया जाएगा कि सुविधाएं इस प्रकार से बनाई गई हों कि गोपनीय जानकारी या गतिविधियां बाहर से दिखाई या सुनाई न दें।
- गोपनीय सूचना प्रसंस्करण सुविधाओं के स्थानों की पहचान करने वाली निर्देशिकाएं और आंतरिक टेलीफोन पुस्तकें किसी भी अनधिकृत व्यक्ति के लिए आसानी से सुलभ नहीं होनी चाहिए।

24.1.4 बाहरी और पर्यावरणीय खतरों से सुरक्षा

प्राकृतिक आपदाओं, दुर्भावनापूर्ण हमलों या दुर्घटनाओं से बचाव के लिए भौतिक सुरक्षा तैयार की जाएगी और उसे लागू किया जाएगा। इसमें निम्नलिखित शामिल होना आवश्यक है:

- विद्युत प्रणालियों को बिना किसी रुकावट के उचित स्तर और गुणवत्ता पर विद्युत उपलब्ध कराने के लिए डिजाइन किया जाएगा;
- अग्नि-शमन प्रणालियों की स्थापना सहित उचित अग्नि सुरक्षा उपायों का कार्यान्वयन;
- बिजली स्रोतों के लिए पर्याप्त अतिरेक सुनिश्चित किया जाना चाहिए और विफलता का कोई भी कारण न हो। जहाँ बिजली स्रोतों का प्रबंधन भवन प्रशासन द्वारा किया जाता है, वहाँ भवन प्रशासन के साथ उचित समझौते किए जाने चाहिए;
- हडको परिसर के अंदर चिन्हित स्थानों पर अग्नि का पता लगाना एवं अलार्म सिस्टम लगाए जाने है;
- सर्वर कक्ष में ज्वलनशील पदार्थों का प्रयोग नहीं किया जाना चाहिए। सर्वर कक्ष में केवल न्यूनतम आवश्यक सामग्री ही रखी जानी चाहिए। पैकिंग सामग्री और अन्य अनावश्यक वस्तुओं को यथाशीघ्र हटा दिया जाना चाहिए;
- सभी कर्मियों को बुनियादी अग्निशमन तकनीकों का प्रशिक्षण दिया जाना चाहिए। कर्मियों की तैयारी की जाँच के लिए समय-समय पर अग्नि अभ्यास आयोजित किए जाएँगे;
- यह आवश्यक है कि तापमान और आर्द्रता की निगरानी और नियंत्रण स्वीकार्य मानकों के अनुसार किया जाए; और
- कीट नियंत्रण और कुतरने वाले जानवरों का नियंत्रण समय-समय पर किया जाता है।

24.1.5 सुरक्षित क्षेत्रों में कार्य करना

- इन क्षेत्रों में उचित व्यक्तिगत पहुंच नियंत्रण लागू किए गए हैं;
- कर्मचारियों को प्रतिबंधित क्षेत्रों तक पहुँच केवल 'आवश्यकता' के आधार पर प्रदान की जाती है;
- प्रतिबंधित क्षेत्रों में किसी भी संपत्ति के प्रवेश और निकास के साथ-साथ आवाजाही की निगरानी और रिकॉर्ड किया जाता है;
- प्रतिबंधित क्षेत्रों में मोबाइल उपकरणों में फोटोग्राफिक, वीडियो, ऑडियो या अन्य रिकॉर्डिंग उपकरण, जैसे गूगल ग्लास, कैमरा आदि की अनुमति नहीं है;
- प्रवेश द्वारों पर उन उपकरणों/उपकरणों की सूची प्रदर्शित की जाती है जिन्हें प्रतिबंधित क्षेत्रों के अंदर ले जाने की अनुमति नहीं है;

24.2 उपकरण

- सभी उपकरणों की निरंतर उपलब्धता और अखंडता सुनिश्चित करने के लिए उनका सही ढंग से रखरखाव किया जाना आवश्यक है।
- सभी उपकरणों (सहायक उपयोगिताओं सहित) को सुरक्षा खतरों और पर्यावरणीय खतरों से भौतिक रूप से संरक्षित किया जाना आवश्यक है।

- आग, बाढ़, भूकंप, विस्फोट, नागरिक अशांति और अन्य प्रकार की प्राकृतिक या मानव निर्मित आपदा से होने वाली क्षति के विरुद्ध भौतिक सुरक्षा डिजाइन लागू की जाएगी।
- विद्युत कटौती के दौरान सेवाओं की निरंतरता सुनिश्चित करने के लिए निर्बाध विद्युत आपूर्ति (यूपीएस) स्थापित करने की आवश्यकता है।

24.2.1 सहायक उपयोगिताएँ

- यह आवश्यक है कि सभी सहायक सेवाएं और प्रक्रियाएं, जैसे कि बिजली, पानी की आपूर्ति, हीटिंग/वेंटिलेशन और एयर कंडीशनिंग, उन सूचना परिसंपत्तियों के लिए पर्याप्त रूप से मापी जाएं जिनका वे समर्थन कर रही हैं और उनका नियमित रूप से निरीक्षण और परीक्षण किया जाता है।
- उपयुक्त विद्युत आपूर्ति प्रदान की जानी चाहिए जो मूल उपकरण निर्माता (ओईएम) विनिर्देश के अनुरूप हो।
- महत्वपूर्ण व्यावसायिक संचालनों का समर्थन करने वाली सूचना परिसंपत्तियों के नियंत्रित शटडाउन या निरंतर कामकाज को समर्थन देने के लिए यूपीएस और जनरेटर स्थापित किए जाएंगे।
- यूपीएस उपकरण और जनरेटर की नियमित रूप से जांच की जाएगी ताकि यह सुनिश्चित किया जा सके कि उनमें पर्याप्त क्षमता और उनका परीक्षण OEM अनुशंसाओं के अनुसार किया गया है।

24.2.2 केबलिंग सुरक्षा

- विद्युत एवं दूरसंचार नेटवर्क केबलों को क्षति या अनधिकृत अवरोधन से सुरक्षित रखा जाएगा।
- सुरक्षित क्षेत्रों के अंदर बिजली और दूरसंचार लाइनें भूमिगत या पर्याप्त रूप से संरक्षित होंगी।
- हस्तक्षेप को रोकने के लिए बिजली के तारों को संचार के तारों से अलग रखा जाएगा।
- केबल रूटिंग और टर्मिनेशन को दर्शाने वाले विस्तृत भौतिक नेटवर्क आरेख सहित दस्तावेज सुविधा प्रमुख या उनके द्वारा नामित कार्मिक के पास होते हैं।
- केबल/डक्ट्स की अनधिकृत प्रवेश के लिए नियमित जांच सुनिश्चित करने हेतु निगरानी प्रक्रियाएं लागू की जानी चाहिए।

24.2.3 उपकरण रखरखाव

- हडको अपने संपूर्ण आईटी परिवेश (डीआर साइटों सहित) के संचालन लचीलापन सुनिश्चित करने के लिए अपनी सूचना प्रणालियों और बुनियादी ढांचे का समर्थन करने हतु एक मजबूत आईटी सेवा प्रबंधन ढांचा स्थापित करेगा।
- कर्तव्यों का प्रभावी पृथक्करण सुनिश्चित करते हुए आईटी संचालनों के प्रबंधन हेतु एक सेवा स्तर प्रबंधन (एसएलएम) प्रक्रिया लागू की जाएगी।

- हडको के परिचालनों के लिए उनकी महत्ता के आधार पर सूचना परिसंपत्तियों की सुरक्षा वर्गीकरण (गोपनीयता, अखंडता और उपलब्धता के संदर्भ में) की पहचान और मानचित्रण हडको सुनिश्चित करेगा।
- व्यावसायिक संचालनों की निर्बाध निरंतरता के लिए, हडको पुराने और असमर्थित हार्डवेयर या सॉफ्टवेयर का उपयोग करने से बचेगा और सॉफ्टवेयर की समर्थन समाप्ति (ईओएस) तिथि और आईटी हार्डवेयर की वार्षिक रखरखाव अनुबंध (एएमसी) तिथियों की निरंतर आधार पर निगरानी करेगा।
- हडको ईओएस तक पहुंचने से पहले हार्डवेयर और सॉफ्टवेयर के प्रतिस्थापन के लिए समयबद्ध तरीके से प्रौद्योगिकी नवीनीकरण योजना विकसित करेगा।

24.2.4 परिसंपत्तियों का निष्कासन

- परिसर के बाहर सूचना परिसंपत्तियों की आवाजाही के लिए, उचित सुरक्षा उपायों का पालन करना आवश्यक है। परिसर के बाहर किसी भी उपकरण की आवाजाही के लिए गेट पास अनिवार्य है।
- संगठन के बाहर जाने वाली सभी परिसंपत्तियों को सामग्री इन/आउट रजिस्टर में ट्रैक किया जाएगा।
- सभी वापसी योग्य परिसंपत्तियों को वापसी तिथि के अनुसार तब तक ट्रैक किया जाना चाहिए जब तक कि परिसंपत्ति संगठन में वापस न आ जाए।
- संगठन के परिसर के अंदर और बाहर आने-जाने वाली आईटी परिसंपत्तियों के अद्यतन रिकॉर्ड को ट्रैक करना और बनाए रखना आईटी विभाग की जिम्मेदारी है।

24.2.5 परिसर के बाहर उपकरणों और परिसंपत्तियों की सुरक्षा

- हडको के स्वामित्व वाले या उसके द्वारा किराये पर लिए गए पोर्टेबल डिवाइस/उपकरण जैसे लैपटॉप, सेलफोन आदि को ले जाने/प्रबंधित करने वाला प्रत्येक उपयोगकर्ता उपकरण की सुरक्षा के लिए जिम्मेदार होगा;
-
- (बैकअप टेप, रिमूवेबल मीडिया आदि) को भौतिक और पर्यावरणीय खतरों के खिलाफ उचित स्तर की सुरक्षा प्राप्त होनी चाहिए;
- कूरियर किए जाने वाले उपकरण/मीडिया को उपकरण/मीडिया को पर्याप्त भौतिक सुरक्षा प्रदान करते हुए पैक किया जाता है;
- संगठन परिसर के बाहर स्थापित उपकरणों की कमीशनिंग के समय और उसके बाद निर्धारित अंतराल पर बुनियादी स्वच्छता जांच की जाती है;
- संगठन परिसर के बाहर स्थापित उपकरणों की निर्दिष्ट अंतराल पर निगरानी की जाएगी;
- यह आवश्यक है कि संगठन के बाहर तदर्थ आधार पर या मरम्मत के लिए ले जाए जाने वाले किसी भी मीडिया या उपकरण के लिए अधिकृत कर्मियों द्वारा हस्ताक्षरित वैध गेट-पास जारी किया जाए; और

- यह सुनिश्चित किया जाएगा कि सभी वापसी योग्य गेट पास का समय-समय पर मिलान किया जाए ताकि यह सुनिश्चित हो सके कि सामग्री उसके इच्छित उपयोग/मरम्मत के बाद वापस कर दी जाए।

24.2.6 अप्राप्य उपयोगकर्ता उपकरण

- सभी हडको कार्मिकों को अपने कार्यस्थल पर उपयोग या संग्रहीत हडको सूचना को डिजिटल और भौतिक प्रारूप में सुरक्षित रखना आवश्यक है।
- सभी हडको कर्मियों को यह सुनिश्चित करना होगा कि उनके कार्यस्थल और अन्य उपकरण उपयोग में न होने पर बंद हों।
- उपयोगकर्ता को अनुप्रयोग या नेटवर्क सेवा के सक्रिय सत्र समाप्त होने पर उन्हें समाप्त/लॉग-ऑफ करना होगा।
- यह सुनिश्चित किया जाएगा कि स्क्रीन को स्वचालित रूप से लॉक करके सिस्टम की सुरक्षा के लिए पासवर्ड संरक्षित स्क्रीनसेवर का उपयोग किया जाए।

24.2.7 क्लिअर डेस्क और क्लिअर स्क्रीन नीति

- यह सुनिश्चित किया जाएगा कि जहां उपयुक्त हो, कागज और कंप्यूटर मीडिया को उपयुक्त लॉक किए गए कैबिनेट और/या अन्य प्रकार के सुरक्षा फर्नीचर में संग्रहित किया जाए, जब उनका उपयोग नहीं हो रहा हो, विशेष रूप से कार्यालय समय के बाद।
- कार्य दिवस के अंत में कर्मचारी से अपेक्षा की जाती है कि वह सभी कार्यालय कागजात और फाइलें अलमारियों में रख दे।
- यह सुनिश्चित किया जाएगा कि गोपनीय और प्रतिबंधित डेटा को सामान्य व्यावसायिक घंटों के बाद खुले में नहीं छोड़ा जाएगा और अनधिकृत पहुंच को रोकने के लिए इसे सुरक्षित स्थान पर रखा जाएगा।
- मुद्रित प्रारूप में गोपनीय और प्रतिबंधित डेटा को संबंधित रिकॉर्ड प्रतिधारण अनुसूची में अवधारण अवधि के अनुसार सुरक्षित श्रेडिंग बिन या पेपर श्रेडर में निपटाया जाना चाहिए।

25 संचालन सुरक्षा

सूचना प्रणालियों और कंप्यूटिंग उपकरणों का प्रभावी और सुरक्षित संचालन सुनिश्चित किया जाना चाहिए। इन सूचना प्रणालियों और कंप्यूटिंग उपकरणों में निहित और/या उनके द्वारा संसाधित सूचना की सुरक्षा के लिए उचित नियंत्रण लागू किए जाने चाहिए।

25.1 संचालन प्रक्रियाएँ और जिम्मेदारियाँ

इसका उद्देश्य सूचना प्रसंस्करण सुविधाओं का सही और सुरक्षित संचालन सुनिश्चित करना है।

❖ **प्रलेखित संचालन प्रक्रियाएँ**

- कार्य में सभी सूचना प्रणालियों, सूचना प्रसंस्करण सुविधाओं और सेवाओं के लिए मानक संचालन प्रक्रिया (एसओपी) विकसित की जानी है जो प्रत्येक विभाग के विभागीय प्रमुखों द्वारा अनुमोदित की जाएगी।
- एसओपी को उपयोगकर्ताओं के लिए उचित स्तर तक विस्तृत रूप से प्रलेखित किया जाएगा। एसओपी में निम्नलिखित शामिल होने चाहिए, लेकिन इन्हीं तक सीमित नहीं:
    - संचालन कार्य जिन्हें निष्पादित करने की आवश्यकता है;
    - त्रुटियों से निपटने के लिए निर्देश और मार्गदर्शन;
    - सिस्टम विफलता की स्थिति में सिस्टम पुनः आरंभ और पुनर्प्राप्ति प्रक्रियाएं;
    - कार्य करने वाले उपयोगकर्ताओं की भूमिकाएं और जिम्मेदारियां;
    - महत्वपूर्ण गतिविधियों के लिए संभावित सुरक्षा निहितार्थ/विचार; और
    - प्रक्रिया दस्तावेज़ में किए गए सभी परिवर्तनों के लिए अनुमोदकों और संस्करण संख्याओं का रिकॉर्ड।
- यह आवश्यक है कि एसओपी की निर्दिष्ट अंतरालों पर समीक्षा की जाए और जब भी कोई संचालन परिवर्तन या प्रणाली परिवर्तन हो, उसे अद्यतन किया जाए। अद्यतन एसओपी को संबंधित विभागाध्यक्ष द्वारा विधिवत अनुमोदित और अद्यतन संस्करण संख्या के साथ जारी किया जाना चाहिए।
- सभी महत्वपूर्ण उपकरणों के लिए तकनीकी गाइड और/या उपयोगकर्ता गाइड पर तीसरे पक्ष से अपडेट की समय-समय पर जांच करें।
- सभी एसओपी केन्द्रीय रूप से स्थित होंगे तथा 'जानने की आवश्यकता' के आधार पर आसानी से उपलब्ध होंगे।

❖ **परिवर्तन प्रबंधन**

यह आवश्यक है कि संगठन, व्यावसायिक प्रक्रियाओं, सूचना प्रसंस्करण सुविधाओं और प्रणालियों में होने वाले उन परिवर्तनों को नियंत्रित किया जाए जो सूचना सुरक्षा को प्रभावित करते हैं।

❖ **क्षमता प्रबंधन**

- हडको यह सुनिश्चित करेगा कि सूचना प्रणालियां और बुनियादी ढांचा व्यावसायिक कार्यों को समर्थन देने में सक्षम हों और सभी सेवा वितरण चैनलों की उपलब्धता सुनिश्चित करें।
- हडको वार्षिक या अधिक नियमित आधार पर आईटी संसाधनों की क्षमता आवश्यकता का सक्रिय रूप से आकलन करेगा। हडको यह सुनिश्चित करेगा कि घटकों, सेवाओं, सिस्टम संसाधनों, सहायक अवसंरचना में आईटी क्षमता नियोजन पिछले रुझानों (अधिकतम उपयोग), वर्तमान व्यावसायिक आवश्यकताओं और आईटी कौशलनीति के अनुसार अनुमानित भविष्य की आवश्यकताओं के अनुरूप हो।
- आईटी क्षमता आवश्यकताओं के मूल्यांकन और मुद्दों के समाधान के लिए उठाए गए कदमों की समीक्षा आईटीएससी द्वारा की जाएगी।

- **विकास, परीक्षण और उत्पादन वातावरण का पृथक्करण**
  परिचालन वातावरण में अनधिकृत पहुंच या परिवर्तन के जोखिम को कम करने के लिए विकास, परीक्षण और परिचालन वातावरण को अलग किया जाएगा।

25.2 मैलवेयर से सुरक्षा

हडको यह सुनिश्चित करे कि आवधिक परीक्षण के माध्यम से सूचना प्रसंस्करण सुविधाओं में दुर्भावनापूर्ण कोड के प्रवेश को रोकने और पता लगाने के लिए आवश्यक सावधानियां लागू की जाएं।

नियंत्रण वायरस, वर्म्स, ट्रोजन और स्पाइवेयर, एडवेयर, स्पैम, रैनसमवेयर और कीस्ट्रोक लॉगर्स जैसे मैलवेयर के कारण हडको के कंप्यूटिंग वातावरण के लिए जोखिमों के प्रबंधन के लिए न्यूनतम आवश्यकता निर्धारित करता है।

हडको अपने संचालन प्रणाली प्रसंस्करण सुविधाओं को सॉफ्टवेयर और वायरस हमलों से बचाने के लिए नियंत्रण निर्धारित करेगा, ताकि आईटी सेवाओं की निर्बाध उपलब्धता सुनिश्चित की जा सके।

इसमें शामिल होंगे:

1. केवल अधिकृत सॉफ़्टवेयर का उपयोग करें
2. सॉफ्टवेयर हमलों से सुरक्षा के लिए प्रौद्योगिकी का उपयोग
3. वायरस हमलों की रिपोर्टिंग और प्रतिक्रिया की प्रक्रिया
4. उपयोगी नीतियाँ
5. पोर्टेबल कंप्यूटरों की सुरक्षा
6. निरंतर प्रशिक्षण

मैलवेयर के विरुद्ध नियंत्रण

- हडको को यह सुनिश्चित करना आवश्यक है कि सभी उपकरणों में दुर्भावनापूर्ण कोड रोकथाम, पहचान और निष्कासन नियंत्रण मौजूद हों। हडको द्वारा अनुमोदित एंटी-मैलवेयर सॉफ़्टवेयर हडको द्वारा प्रबंधित सभी डेस्कटॉप, लैपटॉप और सर्वर पर स्थापित, अद्यतन और कार्यशील होने चाहिए।
- दुर्भावनापूर्ण सॉफ़्टवेयर से सुरक्षा में सहायता के लिए सक्रिय पैचिंग की जाएगी।
- आईटी इन्फ्रास्ट्रक्चर टीम को उन सभी सर्वर, डेस्कटॉप और लैपटॉप पर एंटी-मैलवेयर सॉफ़्टवेयर इंस्टॉल करना आवश्यक है जिनके लिए एंटी-मैलवेयर समाधान उपलब्ध है। आईटी इन्फ्रास्ट्रक्चर टीम को विक्रेता द्वारा पूर्णतः समर्थित एंटी-मैलवेयर सॉफ़्टवेयर इंस्टॉल करना होगा।
- सभी उपकरणों और सर्वरों को उपकरणों की प्रभावी निगरानी के लिए एंटी-वायरस सॉफ़्टवेयर कंसोल को रिपोर्ट करना होगा। आईटी विभाग एंटी-वायरस कंसोल की निगरानी और अनुपालन हेतु सूचना सुरक्षा समिति को रिपोर्ट प्रस्तुत करने के लिए ज़िम्मेदार है। यह आवश्यक है कि समय-समय पर रिपोर्ट तैयार की जाएँ जिनमें निम्नलिखित जानकारी शामिल होनी चाहिए:
  - उन मशीनों की संख्या जहां नवीनतम हस्ताक्षर पैटर्न मौजूद नहीं है।
  - एजेंट लंबे समय तक कंसोल के साथ संचार नहीं करते हैं।

- एंडपॉइंट्स, सर्वरों के लिए अद्यतन परिभाषा कवरेज; और
- नवीनतम मैलवेयर परिभाषाओं को सभी लागू डिवाइसों पर प्रतिदिन या निर्धारित अंतराल पर अद्यतन किया जाएगा।

25.3 सुरक्षित कॉन्फ़िगरेशन दस्तावेज़ और आवधिक मूल्यांकन

कॉन्फ़िगरेशन सुरक्षित कॉन्फ़िगरेशन दस्तावेज़ों पर आधारित होगा। हडको, ओईएम अनुशंसाओं और उद्योगों की सर्वोत्तम प्रचलन आधार पर आधारभूत सुरक्षित कॉन्फ़िगरेशन दस्तावेज़ विकसित करेगा।

एप्लिकेशन सुरक्षा जीवन चक्र

अनुप्रयोगों में इनपुट, आउटपुट और रखरखाव को सुरक्षित करने के लिए नियंत्रण होना चाहिए।

- व्यवसाय-महत्वपूर्ण अनुप्रयोगों के लिए, या तो आपूर्तिकर्ता से स्रोत कोड प्राप्त किया जाना चाहिए या आपूर्तिकर्ता के व्यवसाय से बाहर होने की स्थिति में स्रोत कोड की उपलब्धता सुनिश्चित करने के लिए एक सॉफ्टवेयर एस्क्रो समझौता होना चाहिए।
- कोई भी एप्लिकेशन, i. आपूर्तिकर्ताओं/ओईएम से प्राप्त, ii. ओपन-सोर्स टूल के रूप में उपयोग किया जाता है, या iii. ऑफ-द-शेल्फ खरीदा जाता है, उसे हडको की साइबर सुरक्षा नीति और प्रक्रियाओं के अनुरूप होना चाहिए।
- निर्धारित प्रक्रिया के अनुसार, पूरे अनुप्रयोग जीवनचक्र के दौरान सभी नए और मौजूदा अनुप्रयोगों के लिए सुरक्षित सॉफ्टवेयर विकास जीवनचक्र (सुरक्षित एसडीएलसी) का पालन किया जाना चाहिए।
- स्रोत कोड ऑडिट प्रोफेशनल रूप से सक्षम कर्मियों/सेवा प्रदाताओं द्वारा किया जाना चाहिए या एप्लिकेशन प्रदाताओं/ओईएम से आश्वासन प्राप्त होना चाहिए कि एप्लिकेशन एम्बेडेड दुर्भावनापूर्ण या धोखाधड़ी कोड से मुक्त है।
- आंतरिक/सहयोगात्मक रूप से विकसित अनुप्रयोगों के लिए सुरक्षित कोडिंग प्रचलन को लागू किया जाना चाहिए।
- विकास/अधिग्रहण/कार्यान्वयन के दौरान सिस्टम एक्सेस नियंत्रण, प्रमाणीकरण, लेनदेन प्राधिकरण, डेटा अखंडता, सिस्टम गतिविधि लॉगिंग, ऑडिट ट्रेल, सत्र प्रबंधन, सुरक्षा घटना ट्रैकिंग और अपवाद हैंडलिंग से संबंधित व्यावसायिक कार्यात्मकताओं और सुरक्षा आवश्यकताओं के लिए सिस्टम के प्रारंभिक और चल रहे चरणों में प्रक्रियाओं को स्पष्ट रूप से निर्दिष्ट किया जाना चाहिए।

- व्यावसायिक कार्यात्मकताओं के अलावा, सिस्टम एक्सेस नियंत्रण, प्रमाणीकरण, लेनदेन प्राधिकरण, डेटा अखंडता, सिस्टम गतिविधि लॉगिंग, ऑडिट ट्रेल, सत्र प्रबंधन, सुरक्षा घटना ट्रैकिंग और अपवाद हैंडलिंग से संबंधित सुरक्षा आवश्यकताओं को सिस्टम विकास/अधिग्रहण/कार्यान्वयन के प्रारंभिक और चल रहे चरणों में स्पष्ट रूप से निर्दिष्ट किया जाना चाहिए।
- विकास, परीक्षण और उत्पादन वातावरण को उचित रूप से अलग किया जाना चाहिए।
- सॉफ्टवेयर/अनुप्रयोग विकास दृष्टिकोण खतरा मॉडलिंग पर आधारित होना चाहिए, सुरक्षित कोडिंग सिद्धांतों को शामिल करना चाहिए, और वैश्विक मानकों और सुरक्षित रोलआउट के आधार पर सुरक्षा परीक्षण शामिल करना चाहिए।
- सॉफ्टवेयर/अनुप्रयोग विकास प्रचलन को ओपन वेब एप्लिकेशन सुरक्षा परियोजना (OWASP) जैसे सर्वोत्तम अभ्यास आधार, रेखाओं के आधार पर कमजोरियों को सक्रिय रूप से संबोधित करना चाहिए और एक स्तरित सुरक्षा प्रणाली प्रदान करने के लिए गहन रक्षा के सिद्धांत को अपनाना चाहिए।

- एप्लिकेशन परिवर्तन प्रबंधन - पैच प्रबंधन नीति के अनुसार नवीनतम पैच और हॉटफिक्स के साथ अद्यतन किया जाना चाहिए।

25.4 परिवर्तन और पैच प्रबंधन

हडको निम्नलिखित सुनिश्चित करने हेतु परिवर्तन और पैच प्रबंधन के लिए दस्तावेजी नीतियां और प्रक्रिया लागू करेगा:

- पैच/परिवर्तनों को लागू करने (या किसी विशेष पैच/परिवर्तन अनुरोध को लागू न करने) के व्यावसायिक प्रभाव का आकलन किया जाता है।
- पैच/परिवर्तनों को आवश्यक अनुमोदन के साथ सुरक्षित और समयबद्ध तरीके से लागू/कार्यान्वित और समीक्षा की जाती है।
- किसी एप्लिकेशन सिस्टम या डेटा में कोई भी परिवर्तन वास्तविक व्यावसायिक आवश्यकताओं और अनुमोदनों द्वारा उचित ठहराया गया हो, जो दस्तावेज़ीकरण द्वारा समर्थित हो और एक मजबूत परिवर्तन प्रबंधन प्रक्रिया के अधीन हो; और
- असफल परिवर्तनों/पैच परिनियोजन या अप्रत्याशित हडको परिणामों से उबरने के लिए प्रणाली स्थापित की गई है।

25.5 नेटवर्क प्रबंधन

नेटवर्क सभी परिचालन प्रणाली सुविधाओं के लिए एक महत्वपूर्ण संसाधन है। इसलिए नेटवर्क की सुरक्षा अत्यंत महत्वपूर्ण है। हडको अपने नेटवर्क के माध्यम से प्रवाहित होने वाले नेटवर्क उपकरणों, सेवाओं और डेटा/सूचना की सुरक्षा के लिए व्यापक नियंत्रण स्थापित करेगा। नियंत्रण में निम्नलिखित शामिल होंगे:

- बुनियादी नेटवर्क कनेक्टिविटी
- नेटवर्क उपलब्धता
- ट्रांसमिशन के दौरान सुरक्षा
- तृतीय पक्ष कनेक्टिविटी
- इंटरनेट
- नेटवर्क प्रशासन

25.6 नेटवर्क में पृथक्करण

नेटवर्क को अच्छी नेटवर्क सुरक्षा प्रचलन के अनुरूप डिज़ाइन किया जाएगा। नेटवर्क डिज़ाइन में निम्नलिखित बातों का ध्यान रखा जाएगा।

- सुसंगत तकनीकी मानकों को शामिल करें और सुसंगत नामकरण प्रचलन का समर्थन करें।
- विभिन्न गंभीरता स्तरों वाली प्रणाली को अलग करने के लिए सुरक्षा नेटवर्क क्षेत्र बनाए जाएंगे।
- विफलता के एकल बिंदु और नेटवर्क में प्रवेश बिंदुओं की संख्या को न्यूनतम करना।

हडको नेटवर्क आर्किटेक्चर को स्पष्ट रूप से प्रलेखित किया जाएगा तथा आर्किटेक्चर में परिवर्तनों को प्रतिबिंबित करने के लिए आवश्यकतानुसार अद्यतन किया जाएगा।

25.7 सूचना और सॉफ्टवेयर का आदान-प्रदान

सूचना आदान-प्रदान के विभिन्न नए तरीके उपलब्ध हो गए हैं और नए तरीकों का उपयोग बढ़ रहा है। हडको ने सूचना आदान-प्रदान के नए तरीकों के लिए खुद को तैयार कर लिया है।

हडको निम्नलिखित के लिए नियंत्रण निर्धारित करेगा:

- सूचना और सॉफ्टवेयर विनिमय समझौते
- पारगमन मीडिया की सुरक्षा
- इलेक्ट्रॉनिक मेल की सुरक्षा
- इंटरनेट उपयोग की सुरक्षा
- इलेक्ट्रॉनिक कार्यालय प्रणाली की सुरक्षा
- सूचना विनिमय के अन्य रूप

25.8 आउटसोर्सिंग

परिचालनों के लिए सूचना प्रसंस्करण की प्रकृति में परिवर्तन होने से कुछ कार्यों की आउटसोर्सिंग अपरिहार्य हो जाएगी। हडको को यह सुनिश्चित करना होगा कि उपयोग की जाने वाली सेवाएँ प्रतिष्ठित कंपनियों से हों, जिनका सिद्ध ट्रैक रिकॉर्ड हो और जो गुणवत्ता मानकों के अनुसार कार्य करती हों। जिसमें हडको की आवश्यकताओं को पूरा करने वाला एक उपयुक्त सेवा स्तर समझौता और गैर-प्रकटीकरण समझौता शामिल होना चाहिए। इस संबंध में आईटी आउटसोर्सिंग नीति का पालन किया जाना आवश्यक है।

सूचना सेवाओं की आउटसोर्सिंग के सुरक्षा निहितार्थों और सुरक्षा नियंत्रण आवश्यकताओं को निर्धारित करने के लिए एक जोखिम विश्लेषण अध्ययन किया जाएगा।

25.9 डेटा बैकअप सूचना

25.9.1 सूचना बैकअप

आईटी विभाग सभी सर्वरों और संबंधित डेटाबेस में रखे गए डेटा के लिए बैकअप प्रक्रिया निर्धारित करने के लिए जिम्मेदार है।

आईटी विभाग को नियमित बैकअप की निगरानी करनी होगी। नियुक्त व्यक्ति को बैकअप परीक्षण की प्रक्रिया विकसित करनी होगी और साप्ताहिक आधार पर बैकअप से डेटा पुनर्स्थापित करने की क्षमता का परीक्षण करना होगा। निम्नलिखित सिद्धांतों को ध्यान में रखना आवश्यक है:

- बैकअप मीडिया को अग्निरोधी लॉक में संग्रहित किया जाना चाहिए।
- डेटाबेस का बैकअप हर 24 घंटे में लिया जाता है।

25.9.2 लॉगिंग और निगरानी

25.9.3 इवेंट लॉगिंग

- यह आवश्यक है कि एप्लिकेशन सर्वर, ऑपरेटिंग सिस्टम, डेटाबेस, वेब सर्वर और सुरक्षा उपकरणों सहित सभी महत्वपूर्ण सूचना परिसंपत्तियों पर लॉगिंग सक्षम हो।
- महत्वपूर्ण सिस्टम गतिविधियों को ट्रैक करने के लिए लॉगिंग सक्षम की जानी चाहिए और इसमें कम से कम निम्नलिखित को शामिल करना आवश्यक है:
    - उपयोगकर्ता अकाउंट प्रबंधन;

- विशेष विशेषाधिकार पहुंच सहित विशेषाधिकार प्राप्त उपयोगकर्ता गतिविधियाँ;
- ओएस कॉन्फ़िगरेशन में परिवर्तन;
- प्रमाणीकरण विफलताएं; और
- ऑडिट ट्रेल तक एक्सेस

- सूचना परिसंपत्तियों से संबंधित समस्याओं से संबंधित उपयोगकर्ताओं या सिस्टम प्रोग्रामों द्वारा रिपोर्ट की गई त्रुटियों (अर्थात त्रुटियों) को लॉग किया जाना है।

25.9.4 व्यवस्थापक और ऑपरेटर लॉग

- संग्रहीत लॉग के लिए फ़ाइल अखंडता निगरानी और परिवर्तन पहचान सॉफ़्टवेयर का उपयोग किया जा सकता है ताकि यह सुनिश्चित किया जा सके कि अलर्ट उत्पन्न किए बिना मौजूदा लॉग डेटा को बदला नहीं जा सकता है।
- सूचना प्रणालियों के लॉग की समीक्षा के बाद संबंधित टीम एसपीओसी, शीर्ष प्रबंधन और संबंधित शेयरधारकों को आवधिक रिपोर्ट प्रस्तुत की जानी है।

25.9.5 लॉग जानकारी की सुरक्षा

- लॉग सूचना और लॉगिंग सुविधाओं तक एक्सेस को उपयोगकर्ता आईडी और पासवर्ड जैसे प्रमाणीकरण प्रणाली के उपयोग के माध्यम से अनुमोदित प्रशासनिक कर्मियों तक सीमित रखा जाना है।
- महत्वपूर्ण आईटी प्रणालियों के लिए लॉग फ़ाइल की दूरस्थ प्रतिलिपि द्वितीयक संग्रहण या लॉग सर्वर में रखी जाएगी। लॉग की दूरस्थ प्रतिलिपि के लिए केवल पठन-योग्य एक्सेस ही अधिकृत है।
- जहां भी संभव हो, सिस्टम को अनधिकृत उपयोगकर्ताओं द्वारा लॉग को हटाने से बचने के लिए केंद्रीय सर्वर पर भेजने के लिए कॉन्फ़िगर किया जाएगा।
- लॉग को स्वीकार्य वन-वे हैश एल्गोरिथ्म का उपयोग करके एन्क्रिप्ट किया जा सकता है, ताकि यह सुनिश्चित किया जा सके कि विश्लेषण के लिए द्वितीयक भंडारण में कॉपी करते समय या ऑडिट ट्रेल्स को संरक्षित करते समय लॉग फ़ाइलों में कोई बदलाव न हो।
- लॉग संग्रहण क्षमता को ट्रैक करने के लिए सिस्टम या लॉग सर्वर में अलर्ट कॉन्फ़िगर किए जाने चाहिए। लॉग प्रबंधन टीम द्वारा निवारक कार्रवाई यह सुनिश्चित करने के लिए निर्धारित की जानी चाहिए कि सिस्टम में पिछले रिकॉर्ड ईवेंट के ओवरफ़्लो या ओवरराइटिंग के कारण ईवेंट लॉगिंग विफल न हो।

25.9.6 क्लॉक सिंक्रनाइज़ेशन

एप्लिकेशन, ऑपरेटिंग सिस्टम, डेटाबेस, नेटवर्क और सुरक्षा उपकरणों सहित सभी सूचना प्रणालियों को लॉग की गई घटनाओं का सटीक और पता लगाने योग्य रिकॉर्ड प्रदान करने के लिए एक मानक समय डिवाइस/एनटीपी सर्वर के साथ समय सिंक्रनाइज़ेशन बनाए रखना होगा।

25.10 संचालन सॉफ्टवेयर का नियंत्रण

25.10.1 संचालन प्रणाली पर सॉफ़्टवेयर की स्थापना

यह आवश्यक है कि संचालन प्रणालियों पर सॉफ्टवेयर की स्थापना को नियंत्रित करने के लिए प्रक्रियाएं मौजूद हों:

- सूचना प्रणालियों को व्यापक और सफल परीक्षण के बाद ही तैनात किया जाएगा। परीक्षणों में प्रयोज्यता, अन्य प्रणालियों पर प्रभाव और उपयोगकर्ता-मित्रता से संबंधित परीक्षण-परिदृश्य शामिल होंगे।
- परीक्षण गतिविधियाँ उत्पादन वातावरण से अलग पृथक प्रणालियों पर की जानी हैं।
- तैनाती के दौरान, आईटी विभाग को यह सुनिश्चित करना आवश्यक है कि पर्याप्त लॉगिंग और ऑडिटिंग क्षमताओं को सर्वोत्तम संभव तरीके से कॉन्फ़िगर किया गया है।
- आईटी विभाग को यह सुनिश्चित करना होगा कि सूचना प्रणालियों के पिछले संस्करणों को आकस्मिक उपाय के रूप में बनाए रखा जाए। आईटी विभाग को सभी आवश्यक सूचनाओं, मापदंडों, प्रक्रियाओं, कॉन्फ़िगरेशन विवरणों और सहायक सॉफ़्टवेयर के साथ पिछले संस्करण का संग्रह भी सुनिश्चित करना होगा।
- उत्पादन परिवेश में परिवर्तन लागू करने से पहले रोलबैक कौशलनीति और योजना तैयार की जानी चाहिए।

25.10.2 सॉफ़्टवेयर इंस्टॉलेशन पर प्रतिबंध

- उपयोगकर्ताओं द्वारा सॉफ्टवेयर की स्थापना को नियंत्रित करने वाले नियम स्थापित और कार्यान्वित किए जाएंगे।
- संगठन को यह पहचाने की आवश्यक है कि किस प्रकार के सॉफ्टवेयर इंस्टॉलेशन की अनुमति है (उदाहरण के लिए, मौजूदा सॉफ्टवेयर के लिए अपडेट और सुरक्षा पैच) और किस प्रकार के इंस्टॉलेशन निषिद्ध हैं (उदाहरण के लिए, केवल व्यक्तिगत उपयोग के लिए सॉफ्टवेयर और संभावित रूप से दुर्भावनापूर्ण होने के संबंध में सॉफ्टवेयर की वंशावली अज्ञात या संदिग्ध है)।
- उपयोगकर्ताओं के व्यवस्थापक अधिकार प्रतिबंधित होंगे।
- LAN सेटिंग्स उपयोगकर्ता के लिए किसी भी अनधिकृत संशोधन के लिए उपलब्ध नहीं होनी चाहिए।
- व्यावसायिक आवश्यकता के अनुसार रिमूवेबल मीडिया पोर्ट तक एक्सेस केवल सीमित उपयोगकर्ताओं को ही प्रदान की जानी है।

25.11 सूचना प्रणाली लेखा परीक्षा नियंत्रण

25.11.1 सूचना प्रणाली लेखापरीक्षा नियंत्रण

यह सुनिश्चित करने के लिए कि सूचना सुरक्षा नियंत्रण प्रभावी ढंग से काम कर रहे हैं, सूचना प्रणालियों का लेखा-परीक्षण, कार्यान्वित किए गए नियंत्रणों की स्वतंत्र समीक्षा के लिए किसी बाह्य लेखा परीक्षक द्वारा किया जाएगा।

- निवेश पर जांच से संबंधित लेखापरीक्षा आवश्यकताओं और संबद्धता के पोर्टफोलियो की योजना और संयुक्त उद्यम पर सहमति बनाई जाएगी ताकि व्यावसायिक उद्यमों में लचीलेपन के जोखिम को कम से कम किया जा सके।

- लेखापरीक्षा के दायरे को परिभाषित करने के लिए जोखिम आधारित दृष्टिकोण अपनाया जाएगा।
- यह आवश्यक है कि वार्षिक लेखा परीक्षा अनुसूची, लेखा परीक्षा आवश्यकताएं और लेखा परीक्षा का दायरा संबंधित व्यावसायिक इकाइयों के उपयुक्त प्रतिनिधियों के साथ सहमत हो।
- यह सुनिश्चित किया जाना चाहिए कि जहाँ भी संचालन प्रणाली तक एक्सेस की आवश्यकता हो, वह केवल सॉफ्टवेयर और डेटा तक ही सीमित हो। ऑडिट पूरा होने पर यह एक्सेस हटा दी जानी चाहिए।
- उपरोक्त आवश्यकता के अपवाद केवल सिस्टम फाइलों की पृथक प्रतियों (सिस्टम फाइलों की प्रतियां जो मूल से लिंक नहीं हैं) के लिए ही अनुमत होंगे, जिन्हें ऑडिट पूरा होने पर मिटा दिया जाएगा।
- लेखापरीक्षा प्रक्रियाओं, आवश्यकताओं, जिम्मेदारियों और निष्कर्षों का दस्तावेजीकरण किया जाना है।
- सूचना प्रणाली लेखापरीक्षा उपकरणों (उदाहरण के लिए सॉफ्टवेयर और डेटा) तक एक्सेस को किसी भी संभावित दुरुपयोग या समझौता को रोकने के लिए उचित नियंत्रणों के माध्यम से संरक्षित करने की आवश्यकता है।
- यह सुनिश्चित किया जाएगा कि लेखा परीक्षकों से गैर-प्रकटीकरण समझौता प्राप्त किया जाए।

26 रिमोट एक्सेस

यह सुनिश्चित किया जाएगा कि सूचना सुरक्षा संपूर्ण जीवनचक्र में सूचना प्रणाली का एक अभिन्न अंग है और इसमें सार्वजनिक नेटवर्क पर सेवाएं प्रदान करने वाली सूचना प्रणाली की आवश्यकताएं भी शामिल हैं।

- हडको नियमित रूप से दूरस्थ पहुंच अनुमोदनों की समीक्षा करेगा तथा उन अनुमोदनों को रद्द कर देगा जिनके लिए अब कोई ठोस व्यावसायिक औचित्य नहीं है।
- हडको को रिमोट एक्सेस डिवाइसों पर सभी सॉफ्टवेयरों की उचित समय पर पैचिंग, अद्यतनीकरण और रखरखाव सुनिश्चित करना चाहिए।
- एक्सेस डिवाइस और हडको के बीच महत्वपूर्ण डेटा के संचार की सुरक्षा के लिए एन्क्रिप्शन का उपयोग किया जाना चाहिए।
- VLAN नेटवर्क, सेगमेंट, दिशा-निर्देश और अन्य तकनीकों का उपयोग हडको के भीतर अधिकृत नेटवर्क क्षेत्रों और अनुप्रयोगों तक दूरस्थ एक्सेस को प्रतिबंधित करने के लिए किया जाना चाहिए।
- समय-समय पर एक्सेस डिवाइस कॉन्फ़िगरेशन और पैच स्तरों का ऑडिट करना।
- दूरस्थ एक्सेस संचार को लॉग करना, उनका समय पर विश्लेषण करना और विसंगतियों पर कार्रवाई करना।
- सुसंगत प्रमाणीकरण प्रक्रिया प्रदान करने के लिए मॉडेम और इंटरनेट एक्सेस को केंद्रीकृत करें और इनबाउंड और आउटबाउंड नेटवर्क ट्रैफ़िक को उचित परिधि सुरक्षा और नेटवर्क निगरानी के अधीन करें।
- सभी रिमोट एक्सेस के लिए दिनांक, समय, उपयोगकर्ता, उपयोगकर्ता स्थान, अवधि और उद्देश्य को रिमोट एक्सेस के माध्यम से सभी गतिविधियों सहित लॉग करना और मॉनिटर करना।

- दूरस्थ एक्सेस के लिए दो-कारक प्रमाणीकरण प्रक्रिया की आवश्यकता (एक बार के यादृच्छिक पासवर्ड जनरेटर या टोकन-आधारित पीकेआई के साथ पिन आधारित टोकन कार्ड)
- दूरस्थ उपयोग की संवेदनशीलता के अनुरूप नियंत्रणों का कार्यान्वयन उदाहरण के लिए, संवेदनशील सिस्टम या डेटाबेस को प्रबंधित करने के लिए दूरस्थ उपयोग में नीति और कॉन्फ़िगरेशन द्वारा एक्सेस डिवाइस के उपयोग को प्रतिबंधित करना, एक्सेस डिवाइस के प्रमाणीकरण की आवश्यकता और एक्सेस प्रदान करने से पहले एक्सेस डिवाइस की विश्वसनीयता सुनिश्चित करना जैसे नियंत्रण शामिल हो सकते हैं।

26.1 एप्लिकेशन स्वामी की भूमिका

- एप्लिकेशन में किए जाने वाले किसी भी परिवर्तन को प्राथमिकता देना और परिवर्तनों को अधिकृत करना।
- व्यवसाय मालिकों के साथ समझौते में प्रासंगिक नीतियों के अनुसार किसी एप्लिकेशन से संबंधित डेटा के लिए डेटा वर्गीकरण, डी-वर्गीकरण और अभिलेखीय प्रक्रियाओं पर निर्णय लेना।
- यह सुनिश्चित करना कि अनुप्रयोग के डिजाइन, विकास और परीक्षण में सक्रिय भागीदारी के माध्यम से अनुप्रयोग में पर्याप्त नियंत्रण निर्मित किए गए हैं।
- यह सुनिश्चित करना कि एप्लिकेशन की सुरक्षा की समीक्षा की गई है।
- सुनिश्चित करें कि एक्सेस और भूमिकाओं की समीक्षा समय-समय पर की जाती है।

27 संचार सुरक्षा

27.1 नेटवर्क सुरक्षा प्रबंधन

27.1.1 नेटवर्क एक्सेस नियंत्रण

- यह सुनिश्चित किया जाएगा कि व्यावसायिक आवश्यकताओं की पूर्ति सुनिश्चित करने के लिए सेवा स्तरों के साथ-साथ नेटवर्क सेवाओं की पहचान, दस्तावेजीकरण और अनुमोदन किया जाए।
- नेटवर्क सेवाओं की निगरानी की जानी चाहिए तथा सहमत सेवा स्तरों के सापेक्ष उनके प्रदर्शन को मापने के लिए रिपोर्ट तैयार की जानी चाहिए।
- महत्वपूर्ण नेटवर्क उपकरणों तक एक्सेस को अधिकृत उपयोगकर्ताओं तक सीमित करने के लिए केंद्रीकृत पहुंच नियंत्रण समाधान के माध्यम से प्रबंधित किया जाना है।
- नेटवर्क डायग्नोस्टिक उपकरणों के उपयोग को कड़ाई से नियंत्रित किया जाना चाहिए ताकि अनधिकृत उपयोगकर्ताओं को नेटवर्क के बारे में संवेदनशील जानकारी प्राप्त करने से रोका जा सके।
- केवल अधिकृत उपयोगकर्ताओं को ही लोकल एरिया नेटवर्क का उपयोग करने की अनुमति होगी।
- केवल हडको द्वारा अनुमोदित वायरलेस लोकल एरिया नेटवर्क (WLAN) ही हडको नेटवर्क से जोड़े जा सकते हैं। सभी बाहरी नेटवर्किंग कनेक्शन हडको द्वारा प्रबंधित नेटवर्क इन्फ्रास्ट्रक्चर के माध्यम से किए जाने चाहिए और इसमें नेटवर्क सुरक्षा निगरानी भी शामिल होनी चाहिए।
- प्रबंधन वर्चुअल लोकल एरिया नेटवर्क (VLAN) अन्य VLAN से अलग होगा। जहाँ तक संभव हो, प्रबंधन ट्रैफ़िक को प्रोडक्शन नेटवर्क से होकर नहीं गुजरना चाहिए। यदि इन-बैंड (प्रोडक्शन नेटवर्क पर) संचार आवश्यक हो, तो एसएसएच जैसे एन्क्रिप्टेड संचार प्रोटोकॉल का उपयोग किया जाएगा।

- यह सुनिश्चित किया जाएगा कि हडको नेटवर्क (वायरलेस नेटवर्क सहित) का आर्किटेक्चर आरेख प्रलेखित और अद्यतन रखा जाए। आर्किटेक्चर में किसी भी परिवर्तन (उच्च स्तरीय और निम्न स्तरीय दोनों) की सूचना संबंधित रिपोर्टिंग संरचना के माध्यम से संस्करण नियंत्रण सहित सूचना सुरक्षा विभाग को दी जानी चाहिए।
- हडको परिसर में स्थापित वायरलेस नेटवर्क को कार्यान्वयन से पहले अनुमोदित किया जाएगा। वायरलेस नेटवर्क के लिए सुरक्षित कॉन्फ़िगरेशन, एन्क्रिप्शन और प्रमाणीकरण जैसे नियंत्रण लागू किए जाने हैं। वायरलेस नेटवर्क के प्रबंधन को समग्र नेटवर्क सुरक्षा प्रबंधन में एकीकृत किया जाएगा।
- हडको यह सुनिश्चित करेगा कि नेटवर्क से जुड़ा प्रत्येक वायरलेस उपकरण अधिकृत कॉन्फ़िगरेशन और सुरक्षा प्रोफ़ाइल से मेल खाता हो, कनेक्शन के प्रलेखित स्वामी और परिभाषित व्यावसायिक आवश्यकता के साथ।
- हडको उन वायरलेस उपकरणों तक एक्सेस से इनकार कर देगा जिनमें ऐसा कॉन्फ़िगरेशन और प्रोफ़ाइल नहीं है।
- हडको मोबाइल वाई-फाई उपकरणों जैसे लैपटॉप, आईपैड, मोबाइल उपकरणों और अन्य पोर्टेबल उपकरणों का पता लगाएगा और उन्हें वर्गीकृत करेगा। हडको क्लाइंट मशीनों पर वायरलेस एक्सेस को जहाँ वायरलेस एक्सेस की विशिष्ट व्यावसायिक आवश्यकता की पहचान की गई है, इस प्रकार कॉन्फ़िगर करेगा कि केवल अधिकृत वायरलेस नेटवर्क तक ही एक्सेस की अनुमति हो।
- हडको नियमित रूप से अनधिकृत या गलत तरीके से कॉन्फ़िगर किए गए वायरलेस इंफ्रास्ट्रक्चर उपकरणों की जांच करेगा।
- भेद्यता स्कैनिंग उपकरणों को वायर्ड नेटवर्क से जुड़े वायरलेस एक्सेस पॉइंट्स का पता लगाने के लिए कॉन्फ़िगर किया जाएगा। पहचाने गए उपकरणों का मिलान अधिकृत वायरलेस एक्सेस पॉइंट्स की सूची से किया जाएगा। अनधिकृत (अर्थात, संदिग्ध) एक्सेस पॉइंट्स को निष्क्रिय कर दिया जाएगा।
- हडको, अवैध वायरलेस उपकरणों की पहचान करने और हमले के प्रयासों व सफल घुसपैठ का पता लगाने के लिए वायरलेस घुसपैठ पहचान प्रणालियों (WIDS) का उपयोग करेगा। WIDS के अतिरिक्त, सभी वायरलेस ट्रैफ़िक की निगरानी एक वायर्ड IDS द्वारा की जाएगी क्योंकि ट्रैफ़िक वायर्ड नेटवर्क में प्रवेश करता है।
- हडको यह सुनिश्चित करेगा कि वायरलेस ग्राहक मजबूत, बहु-कारक प्रमाणीकरण क्रेडेंशियल्स का उपयोग करें, ताकि समझौता किए गए क्रेडेंशियल्स से अनधिकृत एक्सेस के जोखिम को कम किया जा सके।
- यह सुनिश्चित किया जाएगा कि किसी अविश्वसनीय नेटवर्क पर हडको नेटवर्क तक दूरस्थ एक्सेस (उदाहरण के लिए वर्चुअल प्राइवेट नेटवर्क (वीपीएन), परिधि फायरवॉल, आदि) को समग्र नेटवर्क सुरक्षा प्रबंधन में एकीकृत किया गया है।
- हडको नेटवर्क में विफलता के सभी एकल बिंदुओं की पहचान की जाएगी और जहाँ तक संभव हो, ऐसे डिज़ाइन में जोखिमों का आकलन किया जाएगा और नेटवर्क विफलता से निपटने के लिए फ़ेलओवर तकनीकें लागू की जानी चाहिए।

- महत्वपूर्ण नेटवर्क उपकरणों के लिए लोड संतुलन समाधान लागू किया जाएगा ताकि उपकरणों से प्रभावी प्रदर्शन सुनिश्चित किया जा सके।
- यह सुनिश्चित किया जाएगा कि नेटवर्क प्रौद्योगिकियों के बैक-अप की व्यवस्था निम्नलिखित के लिए हो:
    - यदि ऐसी जानकारी खो जाती है तो 'वर्तमान' कॉन्फ़िगरेशन को शीघ्रता और सटीकता से पुनः बनाने की आवश्यकता (जहाँ 'वर्तमान' विफलता से पहले ज्ञात अंतिम कॉन्फ़िगरेशन को संदर्भित करता है);
    - कॉन्फ़िगरेशन में परिवर्तन; और
    - इस कॉन्फ़िगरेशन जानकारी का सुरक्षित रखरखाव
- महत्वपूर्ण नेटवर्क उपकरणों द्वारा उत्पन्न लॉग का विश्लेषण खतरों और अपवादों की पहचान करने के लिए किया जाएगा।
- खतरों पर तत्काल प्रतिक्रिया प्रदान करने के लिए नेटवर्क सुरक्षा की निगरानी की जा सकती है।
- हडको नेटवर्कों के बीच ट्रैफ़िक प्रवाह की आवश्यकताओं की पहचान और दस्तावेज़ीकरण किया जाना है। इन नेटवर्कों से गुजरने वाले इनबाउंड और आउटबाउंड ट्रैफ़िक को हडको द्वारा प्रबंधित सुरक्षा तकनीकों, जैसे फ़ायरवॉल और/या आईडीएस/आईपीएस, के माध्यम से फ़िल्टर और/या रूट किया जाएगा।

27.1.2 नेटवर्क सेवाओं की सुरक्षा

- प्रत्येक अविश्वसनीय नेटवर्क से कनेक्शन पर, तथा अर्ध-विश्वसनीय और विश्वसनीय/अत्यधिक विश्वसनीय नेटवर्क के बीच फ़ायरवॉल लागू किया जाएगा।
- इन नेटवर्कों से गुजरने वाले ट्रैफ़िक को और अधिक नियंत्रित करने के लिए आईडीएस/आईपीएस समाधान के माध्यम से गहन सुरक्षा लागू की जाएगी। इन समाधानों को खतरों के वर्तमान संकेतों/विशेषताओं के साथ नियमित रूप से अद्यतन किया जाना चाहिए।
- सभी को अस्वीकार करने का नियम लागू किया जाना है, अर्थात सभी सेवाएं डिफ़ॉल्ट रूप से अक्षम कर दी जाएंगी तथा आवश्यकतानुसार केस-दर-केस आधार पर सेवाओं को चुनिंदा रूप से सक्षम किया जाएगा।
- व्यावसायिक उद्देश्यों के लिए आवश्यक न होने वाली नेटवर्क सेवाएँ, प्रोटोकॉल और पोर्ट अक्षम या बंद कर दिए जाएँगे। केवल औपचारिक रूप से स्वीकृत सेवाएँ ही सक्रिय की जाएँगी।
- जिन्हें नेटवर्क पर सक्षम किया जाएगा उन अनुमोदित सेवाओं की सूची की पहचान, दस्तावेजीकरण और अनुमोदन किया जाना है।
- यह आवश्यक है कि नेटवर्क ट्रैफिक पर लगातार नजर रखी जाए और यदि कोई अस्वीकृत सेवा सक्षम पाई जाती है, तो उसे निष्क्रिय कर दिया जाए।
- फ़ाइल ट्रांसफ़र (एफ़टीपी) और टेलनेट जैसे ज्ञात असुरक्षित प्रोटोकॉल हडको-प्रबंधित नेटवर्क तकनीकों पर लागू नहीं हैं। इस आवश्यकता के अपवादों के लिए, व्यावसायिक औचित्य और सूचना सुरक्षा समिति की मंज़ूरी प्राप्त करनी होगी। यह सुनिश्चित किया जाएगा कि इन प्रोटोकॉल से जुड़े जोखिमों को कम करने के लिए सुरक्षा नियंत्रण लागू किए जाएँ।

- हडको और तीसरे पक्ष के नेटवर्क को आपस में जोड़ने के सुरक्षा और व्यावसायिक निहितार्थों पर विचार करते समय निम्नलिखित बातों को शामिल करना आवश्यक है:
    - सूचना प्रणालियों में कमजोरियां जहां संगठन के विभिन्न हिस्सों के बीच सूचना साझा की जाती है;
    - सूचना साझाकरण को प्रबंधित करने के लिए उपयुक्त नियंत्रण; और
    - चयनित व्यक्तियों से संबंधित जानकारी तक एक्सेस को प्रतिबंधित करना, जैसे संवेदनशील परियोजनाओं पर काम करने वाले कर्मचारी।
- नेटवर्क शेयरिंग प्रोटोकॉल (जैसे SMB V1) का उपयोग न्यूनतम किया जाना चाहिए।

27.1.3 नेटवर्क में पृथक्करण

- यह सुनिश्चित किया गया कि नेटवर्क को सेवा एड्रेस के एक सुपरिभाषित ब्लॉक से प्रदर्शित किया जाए, ताकि एड्रेस के जर्नल में शामिल होने वाले को रुकावट कर सके।
- नेटवर्क को कार्य और संभवतः स्थान के आधार पर सबनेट में विभाजित किया जाना है।
- प्रत्येक नेटवर्क को व्यवसाय और सुरक्षा आवश्यकताओं के आधार पर अलग-अलग वीएलएएन में विभाजित किया जाएगा।
- यह सुनिश्चित किया जाएगा कि हडको नेटवर्क को वेब, एप्लिकेशन या डेटाबेस के रूप में ज़ोन में वर्गीकृत किया जाए। ज़ोन के वर्गीकरण के लिए निम्नलिखित मानदंड का उपयोग किया जाएगा:
    - प्रत्येक नेटवर्क से जुड़ा विश्वास का स्तर; और
    - नेटवर्क पर संग्रहीत या नेटवर्क से गुजरने वाली सूचना की संवेदनशीलता।
- सार्वजनिक रूप से सुलभ प्रणालियाँ, अर्थात्, अविश्वसनीय नेटवर्क (जैसे वेब सर्वर) से सुलभ हडको प्रणालियाँ हडको अर्ध-विश्वसनीय नेटवर्क पर स्थित होंगी।
- विश्वसनीय और अत्यधिक विश्वसनीय नेटवर्कों में केवल अनुमोदित कनेक्शनों की अनुमति देने के लिए राज्य-पूर्ण निरीक्षण लागू किया जाएगा।

27.2 सूचना हस्तांतरण

27.2.1 सूचना हस्तांतरण नीतियां और प्रक्रियाएं

- सूचना ऑनर प्राप्तकर्ता पक्षों को परिभाषित करने के लिए ज़िम्मेदार होगा। यह सुनिश्चित किया जाएगा कि व्यावसायिक आवश्यकताओं के आधार पर सूचना का आदान-प्रदान विभिन्न कार्यों में किया जाए।
- कार्मिकों को सार्वजनिक स्थान पर फोन पर या किसी सहकर्मी के साथ संवेदनशील जानकारी पर चर्चा नहीं करनी चाहिए, जब तक कि उन्होंने यह सावधानी न बरती हो कि उनकी बात न सुनी जाए या उन्हें रोका न जाए।

27.2.2 सूचना हस्तांतरण पर समझौते

- हडको और तीसरे पक्ष के बीच यह सुनिश्चित किया जाएगा कि सूचना/सॉफ्टवेयर के आदान-प्रदान के लिए एक समझौता स्थापित और अच्छी तरह से प्रलेखित हो।

- विनिमय समझौतों को निम्नलिखित सुरक्षा विचारों में संबोधित किया जाएगा:

    - संचरण, प्रेषण और प्राप्ति के बारे में नियंत्रण और अधिसूचना के लिए प्रबंधन की जिम्मेदारियां;
    - इलेक्ट्रॉनिक सूचना केवल संगठन के ई-मेल पर ही साझा की जानी है;
    - इलेक्ट्रॉनिक सूचना को ई-मेल पर भेजते समय एन्क्रिप्ट किया जाना है;
    - कागज़ के रूप में सूचना अनुमोदित कूरियर एजेंसी के माध्यम से भेजी जाएगी;
    - सूचना सुरक्षा संबंधी घटनाओं, जैसे डेटा की हानि, की स्थिति में जिम्मेदारियां और दायित्व;
    - संवेदनशील या महत्वपूर्ण जानकारी के लिए एक सहमत लेबलिंग प्रणाली का उपयोग, यह सुनिश्चित करना कि लेबल का अर्थ तुरंत समझ में आ जाए और जानकारी को उचित रूप से संरक्षित किया जाए; और
    - डेटा संरक्षण, कॉपीराइट, सॉफ्टवेयर लाइसेंस अनुपालन और इसी तरह के विचारों के लिए स्वामित्व और जिम्मेदारियां।

27.2.3 इलेक्ट्रॉनिक संदेश

हडको ईमेल संसाधनों का निम्नलिखित उपयोग निषिद्ध/अस्वीकार्य माना गया है:

- निम्नलिखित विशेषताओं वाले ईमेल भेजना:

    - ऐसे फ़ाइल एक्सटेंशन वाले अटैचमेंट जो मैलवेयर के लिए अतिसंवेदनशील होते हैं। उदाहरण के लिए, .exe, .vb, .vbs और .com
    - ऐसे अटैचमेंट जिनमें गैर-व्यावसायिक जानकारी हो, जैसे संगीत या वीडियो फ़ाइलें
    - मैलवेयर युक्त
    - स्पैम या फ़िशिंग के रूप में समझी गई जानकारी
    - ऐसे ईमेल जिन्हें मानव संसाधन या समान कार्य द्वारा अस्वीकार्य माना जाता है
    - धोखाधड़ी और श्रृंखलाबद्ध ईमेल वितरित करना
    - जब तक किसी विशेष उपयोगकर्ता को विशेष रूप से निर्दिष्ट न किया जाए, उपयोगकर्ता को हडको के भीतर या बाहर किसी अन्य व्यक्ति के लिए लक्षित ईमेल को रोकना या प्रकट नहीं करना चाहिए।

  - किसी भी प्रकार की मेल स्पूफिंग में शामिल होना, जिसमें मेल भेजने का प्रयास करना शामिल है, जिससे ऐसा प्रतीत हो कि उसका स्रोत कोई अन्य उपयोगकर्ता या मशीन, या कोई अस्तित्वहीन मशीन है।
  - गैर-व्यावसायिक मामलों से संबंधित प्राप्तकर्ताओं की एक बड़ी सूची को भेजना, अग्रेषित करना और/या उत्तर देना।
- हडको ईमेल संसाधनों का समस्त उपयोग संगठन के सामग्री फ़िल्टरिंग नियमों के अधीन है।
- हडको की ईमेल प्रणाली का उपयोग किसी भी विघटनकारी या आपत्तिजनक संदेशों के निर्माण या वितरण के लिए नहीं किया जाना चाहिए, जिसमें जाति, लिंग, बाल, रंग, विकलांगता, आयु, यौन अभिविन्यास, अश्लील साहित्य, धार्मिक विश्वास और अभ्यास, राजनीतिक विश्वास, या/और राष्ट्रीय मूल आदि के बारे में आपत्तिजनक टिप्पणियां शामिल हैं। जिन कार्मिकों को किसी अन्य कार्मिक से इस प्रकार की सामग्री वाला कोई ईमेल प्राप्त होता है, उन्हें सूचना सुरक्षा समिति को मामले की रिपोर्ट करना आवश्यक है।
- हडको से किसी बाहरी नेटवर्क पर कोई भी ईमेल भेजते समय कार्मिकों को अत्यधिक सावधानी बरतनी चाहिए। संवेदनशील जानकारी किसी भी माध्यम से अग्रेषित नहीं की जानी चाहिए, जब तक कि वह ईमेल व्यवसाय के लिए महत्वपूर्ण न हो और एन्क्रिप्टेड न हो।
- किसी भी विशेष विशेषाधिकार के लिए सूचना सुरक्षा प्रमुख का अनुमोदन आवश्यक है। यह सुनिश्चित किया जाएगा कि ऐसी किसी भी गतिविधि का लॉग सूचना सुरक्षा समिति को भेजा जाए।
- गैर-व्यावसायिक ईमेल अकाउंट का उपयोग हडको सूचना प्राप्त करने या भेजने के लिए नहीं किया जाएगा।
- जिन उपयोगकर्ताओं को स्पैम या फ़िशिंग ईमेल प्राप्त होते हैं, उन्हें तुरंत सूचना सुरक्षा समिति को सूचित करना होगा और इसकी रिपोर्ट करनी होगी।
- हडको द्वारा प्रदान किए गए ईमेल अकाउंट के उपयोगकर्ता, हडको के भीतर या बाहर अन्य उपयोगकर्ताओं को उनके अकाउंट से भेजे गए, उत्तर दिए गए या अग्रेषित किए गए ईमेल की सामग्री के लिए पूरी तरह से जिम्मेदार होंगे।
- उपयोगकर्ताओं को अपना ईमेल अकाउंट या अन्य जानकारी वेबसाइटों या किसी अन्य इंटरनेट फोरम जैसे मेलिंग सूची या सोशल नेटवर्किंग वेबसाइट को प्रदान करने में सावधानी बरतनी चाहिए।
- संगठन के ईमेल सिस्टम से वायरस या अन्य मैलवेयर चेतावनियाँ और सामूहिक मेल भेजने से पहले विभाग प्रमुखों/प्रबंधकों द्वारा अनुमोदित होना आवश्यक है। ये प्रतिबंध हडको कर्मचारी द्वारा प्राप्त मेल के अग्रेषण पर भी लागू होंगे।
- हडको के कार्मिकों को कंपनी के ईमेल सिस्टम पर संग्रहीत, भेजी या प्राप्त की गई किसी भी चीज़ में गोपनीयता की कोई अपेक्षा नहीं है। संगठन बिना किसी पूर्व सूचना के संदेशों की निगरानी कर सकता है।
- हडको द्वारा केवल अनुमोदित त्वरित संदेश सेवाओं का ही उपयोग किया जाना है।

28 सिस्टम विकास, अधिग्रहण और रखरखाव

28.1 सूचना प्रणालियों की सुरक्षा आवश्यकताएँ

28.1.1 सूचना सुरक्षा आवश्यकताओं का विश्लेषण और विनिर्देश

- व्यावसायिक आवश्यकता के आधार पर, अनुरोधकर्ता (प्रबंधन या व्यावसायिक उपयोगकर्ता) को अपनी कार्यक्षमता आवश्यकता की समझ के आधार पर, पूर्वनिर्धारित टेम्पलेट पर अपनी आवश्यकताओं को आईटी विभाग को प्रस्तुत करना आवश्यक है।
- संबंधित विभाग प्रमुखों को व्यवहार्यता अध्ययन के बाद इस प्रस्ताव का मूल्यांकन करना होगा। इस अध्ययन में निम्नलिखित शामिल होने चाहिए:
    - वर्तमान कमियाँ
    - अपेक्षित लाभ
    - सॉफ्टवेयर द्वारा प्रदान की जाने वाली कार्यात्मक आवश्यकताएं।
    - बाजार में उपलब्ध वैकल्पिक ऑफ-द-शेल्फ उत्पाद और समाधान; और
    - समाधान विकसित करने के लिए आवश्यक मानवशक्ति और अन्य सॉफ्टवेयर/हार्डवेयर के संदर्भ में अनुमानित लागत।
- प्रस्ताव की सुरक्षा और अनुपालन सुनिश्चित करने के लिए परियोजना प्रबंधकों और अन्य विभाग प्रमुखों को सूचना सुरक्षा समिति की जानकारी में रखा जाएगा।
- व्यवहार्यता अध्ययन रिपोर्ट का लागत और लाभ के संदर्भ में विश्लेषण किया जाना है और निम्नलिखित में से कोई भी निर्णय लिया जा सकता है:-
    - उत्पाद का विकास (इन-हाउस या आउटसोर्स्ड) करना।
    - कमर्शियल ऑफ-द-शेल्फ (COTS) उत्पाद खरीदें।
    - उत्पाद खरीदें और अनुरोध को अनुकूलित करें या अस्वीकार करें।
- परियोजना प्रबंधकों और विभागाध्यक्षों को प्रस्तावित समाधान की मौजूदा अनुप्रयोग और वातावरण के साथ अंतर-संचालनीयता का आकलन करना आवश्यक है।

28.2 विकास और समर्थन प्रक्रियाओं में सुरक्षा

28.2.1 सुरक्षित विकास नीति

- सुरक्षा आवश्यकताओं को डिज़ाइन स्तर के दौरान शामिल किया जाएगा।
- परियोजना के अंतर्गत सुरक्षा जांच बिन्दुओं की समीक्षा की जाएगी और उनका दस्तावेजीकरण किया जाएगा।
- यह आवश्यक है कि डेवलपर्स यह सुनिश्चित करें कि विकास प्रक्रिया के दौरान उद्योग की सर्वोत्तम प्रचलित और अनुप्रयोग सुरक्षा मानकों जैसे कि ओपन वेब अनुप्रयोग सुरक्षा परियोजना (OWASP) का पालन किया जाए।
- संस्करण नियंत्रण का पालन किया जाना चाहिए और रिपॉजिटरी को सुरक्षित किया जाना चाहिए।

28.2.2 सॉफ़्टवेयर पैकेजों में परिवर्तन पर प्रतिबंध

- विक्रेता द्वारा आपूर्ति किये गए सॉफ्टवेयर पैकेजों को विक्रेता से परामर्श किये बिना यथासंभव संशोधित नहीं किया जाना चाहिए।
- ऐसे सॉफ्टवेयर में परिवर्तन की किसी भी आवश्यकता को नियंत्रित किया जाएगा तथा परिवर्तन प्रबंधन प्रक्रिया से गुजरना होगा।
- यदि परिवर्तन आवश्यक हों, तो मूल सॉफ्टवेयर को बरकरार रखा जाना चाहिए, तथा परिवर्तन स्पष्ट रूप से पहचानी गई प्रतिलिपि पर लागू किए जा सकते हैं।

28.2.3 सुरक्षित सिस्टम इंजीनियरिंग सिद्धांत

- सुरक्षा इंजीनियरिंग सिद्धांतों पर आधारित सुरक्षित सूचना प्रणाली इंजीनियरिंग प्रक्रियाओं को स्थापित, प्रलेखित और आंतरिक सूचना प्रणाली इंजीनियरिंग गतिविधियों पर लागू किया जाएगा।
- यह आवश्यक है कि सुरक्षा को सभी आर्किटेक्चर परतों (व्यवसाय, डेटा, अनुप्रयोग और प्रौद्योगिकी) में डिज़ाइन किया जाए, जिससे सूचना सुरक्षा की आवश्यकता और एक्सेस की आवश्यकता के बीच संतुलन बना रहे।
- नई तकनीकी सुरक्षा जोखिमों के लिए विश्लेषण किया जाना चाहिए और ज्ञात आक्रमण पैटर्न के आधार पर डिज़ाइन की समीक्षा की जानी चाहिए। इन सिद्धांतों और स्थापित इंजीनियरिंग प्रक्रियाओं की नियमित रूप से समीक्षा की जानी चाहिए ताकि यह सुनिश्चित किया जा सके कि वे इंजीनियरिंग प्रक्रिया के भीतर सुरक्षा के उन्नत मानकों में प्रभावी रूप से योगदान दे रहे हैं।
- यह सुनिश्चित किया जाएगा कि उनकी नियमित रूप से समीक्षा की जाए ताकि वे किसी भी नए संभावित खतरों से निपटने के मामले में अद्यतन रहें और लागू की जा रही प्रौद्योगिकियों और समाधानों में प्रगति के लिए उपयुक्त बने रहें।
- स्थापित सुरक्षा इंजीनियरिंग सिद्धांतों को, जहां लागू हो, संगठन और आपूर्तिकर्ता, जिसे संगठन आउटसोर्स करता है, के बीच अनुबंधों और अन्य बाध्यकारी समझौतों के माध्यम से आउटसोर्स की गई सूचना प्रणालियों पर लागू किया जाएगा।

28.2.4 सुरक्षित विकास वातावरण

- विभिन्न विकास परिवेशों जैसे परीक्षण, विकास और उत्पादन के बीच पृथक्करण सुनिश्चित किया जाना है।
- विकास पर्यावरण तक एक्सेस पर प्रतिबंध आवश्यकता के आधार पर होना चाहिए।
- विकास परिवेश से और उसमें डेटा की आवाजाही को नियंत्रित किया जाएगा।

28.2.5 संचालन प्रणालियों की सिस्टम फ़ाइलों में सुरक्षा

सुरक्षा नीतियाँ इस प्रकार परिभाषित की जाएँगी कि सिस्टम सॉफ़्टवेयर फ़ाइलों और सिस्टम कॉन्फ़िगरेशन डेटा के वितरण को नियंत्रित और मॉनिटर किया जाए ताकि उनकी अखंडता और उपलब्धता सुनिश्चित हो सके और अधिकृत एक्सेस को रोका जा सके। ऑपरेशनल सिस्टम फ़ाइलों को विकास और परीक्षण प्रणालियों से अलग भी रखा जाना चाहिए।

28.2.6 सार्वजनिक नेटवर्क पर एप्लिकेशन सेवाओं को सुरक्षित करना

हडको द्वारा सार्वजनिक नेटवर्क पर प्रसारित की जाने वाली अनुप्रयोग सेवाओं में सम्मिलित सभी सूचनाओं को किसी भी धोखाधड़ीपूर्ण गतिविधि, अनुबंध विवाद, अनधिकृत प्रकटीकरण, तथा संशोधन और/या विनाश से सुरक्षित रखा जाएगा।

28.2.7 आउटसोर्स विकास

- सूचना प्रणालियों का अधिग्रहण अनुमोदित खरीद नीति के अनुसार किया जाएगा।
- व्यवहार्यता अध्ययन का मूल्यांकन करने के बाद, परियोजना प्रबंधकों और विभागाध्यक्षों विभागाध्यक्षों को आवश्यक कार्यक्षमता दस्तावेज के साथ विभिन्न विक्रेताओं तक पहुंचकर सूचना प्रणाली अधिग्रहण के साथ आगे बढ़ना होगा।
- परियोजना प्रबंधकों और क्रय समिति को विक्रेता मूल्यांकन करना आवश्यक है।
- हडको की प्राथमिकताओं, बाधाओं, जोखिम सहनशीलता और मान्यताओं को स्थापित किया जाना है और आपूर्ति श्रृंखला जोखिमों के प्रबंधन से जुड़े निर्णयों के समर्थन में उनका उपयोग किया जाना है। हडको को आपूर्ति श्रृंखला जोखिमों की पहचान, आकलन और प्रबंधन हेतु प्रक्रियाओं को स्थापित और कार्यान्वित करना है।
- साइबर सुरक्षा आपूर्ति श्रृंखला जोखिम प्रबंधन कौशलनीति/प्रक्रिया की पहचान, स्थापना, मूल्यांकन, प्रबंधन और संगठनात्मक शेयरधारकों द्वारा सहमति दी जाएगी।
- सूचना प्रणालियों, घटकों और सेवाओं के आपूर्तिकर्ताओं और तृतीय-पक्ष सेवा प्रदाताओं की पहचान, प्राथमिकता और मूल्यांकन साइबर-आपूर्ति श्रृंखला जोखिम मूल्यांकन प्रक्रिया का उपयोग करके किया जाएगा।
- इस प्रक्रिया का उद्देश्य यह होगा कि हडको एक व्यापक विक्रेता जोखिम मूल्यांकन प्रक्रिया स्थापित करेगा और पहचाने गए जोखिम और भौतिकता के अनुपात में नियंत्रण लागू करेगा:

    - सांद्रता जोखिमों को कम करना
    - हितों के मतभेद को रोकना या उनका समाधान करना
    - विफलता के एकल बिंदुओं से जुड़े जोखिमों को कम करना
    - ग्राहक डेटा सुरक्षा के लिए लागू कानूनी, नियामक आवश्यकताओं और मानकों का अनुपालन सुनिश्चित करना
    - निर्बाध ग्राहक सेवा सुनिश्चित करने के लिए उच्च उपलब्धता बनाए रखना तथा आपूर्ति श्रृंखला जोखिमों का प्रभावी ढंग से प्रबंधन करना।

- अधिग्रहीत की जाने वाली सूचना प्रणालियों का मूल्यांकन निम्नलिखित के आधार पर किया जाएगा:

- व्यावसायिक आवश्यकता के लिए व्यवहार्यता
- विक्रेता प्रतिबद्धता;
- विक्रेता प्रतिबद्धता;
- वाणिज्यिक विचार;
- तकनीकी कौशल; और
- सूचना सुरक्षा आवश्यकता को पूरा करने की क्षमता

- सॉफ्टवेयर में उपयुक्त सत्यापन नियंत्रण (इनपुट और आउटपुट) और सूचना प्रसंस्करण नियंत्रण अंतर्निहित हैं।
- डेटा की उचित सुरक्षा प्रदान करने के लिए सॉफ्टवेयर में पर्याप्त क्रिप्टोग्राफिक और कुंजी प्रबंधन नियंत्रण स्थापित किए गए हैं।
- सुरक्षा कमियों की जांच के लिए सॉफ्टवेयर कोड का आंतरिक मूल्यांकन किया जाता है।
- विक्रेता को अंतिम रूप देने पर, अधिग्रहण चेकलिस्ट के भाग के रूप में, आईटी विभाग को यह पुष्टि करने की आवश्यकता होती है कि विक्रेता निम्नलिखित न्यूनतम आवश्यकताएं प्रदान करते हैं:
    - सॉफ्टवेयर विवरण (खरीदा गया मॉड्यूल/सूट).
    - प्रमाणीकरण (उपयोगकर्ता आईडी, एलडीएपी/सक्रिय निर्देशिका)
    - हार्डवेयर आवश्यकताएँ (सर्वर, रैम, क्लाइंट आवश्यकताएँ)
    - आर्किटेक्चर (क्लाइंट-सर्वर/वेब/वर्चुअलाइजेशन)
    - नेटवर्क आवश्यकताएँ (लैन/वैन, फ़ायरवॉल, पोर्ट, प्रोटोकॉल विवरण)
    - डेटाबेस आवश्यकताएँ
    - सहायक दस्तावेज (सॉफ्टवेयर मैनुअल)

- अधिग्रहीत सॉफ्टवेयर को परिसंपत्ति रजिस्टर में अद्यतन किया जाना चाहिए, जिसमें नाम, विक्रेता, लाइसेंस विवरण (लाइसेंस संख्या और समाप्ति की तारीख) और समर्थन सेवा विवरण (सेवा संपर्क, स्थान और एस्केलेशन मैट्रिक्स) का विवरण दिया जाना चाहिए।

- विक्रेता द्वारा तृतीय पक्ष जोखिम प्रबंधन प्रक्रिया के अनुसार सूचना सुरक्षा प्रश्नावली विधिवत भरी जाएगी।

28.2.8 सिस्टम सुरक्षा परीक्षण

- यह आवश्यक है कि हडको विकास प्रक्रियाओं के दौरान संपूर्ण परीक्षण और सत्यापन सुनिश्चित करे, जिसमें गतिविधियों की विस्तृत सूची तैयार करना भी शामिल है।
- नवीनतम और अद्यतन प्रणालियों को विकास प्रक्रियाओं के दौरान गहन परीक्षण और सत्यापन की आवश्यकता होती है, जिसमें विभिन्न परिस्थितियों के तहत गतिविधियों और परीक्षण इनपुट और अपेक्षित आउटपुट की विस्तृत अनुसूची तैयार करना शामिल है।

- ऐसे परीक्षण शुरुआत में विकास टीम द्वारा आंतरिक विकास के लिए किए जाने चाहिए। इसके बाद स्वतंत्र स्वीकृति परीक्षण (आंतरिक और आउटसोर्स किए गए विकास दोनों के लिए) किया जाना चाहिए ताकि यह सुनिश्चित हो सके कि सिस्टम अपेक्षानुसार और केवल अपेक्षानुसार ही काम करता है।
- इसके बाद उपयोगकर्ता स्वीकृति परीक्षण किया जाएगा ताकि यह सुनिश्चित किया जा सके कि सिस्टम अपेक्षानुसार काम कर रहा है।
- उत्पादन में तैनाती से पहले यह आवश्यक है कि नए एप्लिकेशन और सेवाओं के पास भेद्यता मूल्यांकन स्कैन रिपोर्ट हो, जो विक्रेता द्वारा उपलब्ध कराई जाती है।

28.3 परीक्षण डेटा

28.3.1 परीक्षण डेटा की सुरक्षा

- सभी परीक्षण डेटा, अस्थायी अकाउंट और व्यक्तिगत पहचान योग्य जानकारी (PII) सहित अस्थायी पासवर्ड, उत्पादन परिवेश में तैनात करने से पहले सिस्टम से हटा दिए जाएँगे। इसके अलावा, जहाँ भी संभव हो, सामान्य अकाउंट भी हटा दिए जाएँगे।
- परीक्षण वातावरण को उत्पादन वातावरण के समान सामान्य नियंत्रण वातावरण के अंतर्गत प्रबंधित किया जाएगा।
- परीक्षण डेटा का चयन सावधानीपूर्वक किया जाएगा, तथा उसे संरक्षित और नियंत्रित किया जाएगा।

29 आपूर्तिकर्ता सेवा वितरण प्रबंधन

29.1 आपूर्तिकर्ता सेवाओं की निगरानी और समीक्षा

- आपूर्तिकर्ता द्वारा प्रदान की गई सेवा रिपोर्ट और साक्ष्यों की नियमित अंतराल पर समीक्षा की जानी चाहिए।
- आपूर्तिकर्ता ऑडिट ट्रेल्स और सुरक्षा घटनाओं, परिचालन समस्याओं, विफलताओं, दोष लॉगिंग और व्यवधानों के रिकॉर्ड की समीक्षा नियमित रूप से की जाएगी।
- संबंधित विभागों को विधिक एवं क्रय विभाग के परामर्श से, सेवा स्तर समझौते (एसएलए) में किसी भी अपवाद की स्थिति में सेवा स्तर समझौते की समीक्षा करनी होगी। समीक्षा के दौरान निम्नलिखित पहलुओं पर विचार किया जाएगा:
    - सेवाओं से संबंधित समस्याएं;
    - सेवा प्रवृत्तियों की पहचान;
    - यदि सेवा स्तर सहमत एसएलए को पूरा नहीं करते हैं, तो सुधार के लिए कार्रवाई की जाती है;
    - सेवाओं के दायरे में परिवर्तन;
    - सेवा स्तरों की स्वीकार्य सीमा;
    - निगरानी या रिपोर्टिंग प्रक्रियाओं में परिवर्तन; और
    - दंड संरचना में परिवर्तन

- सेवा में किसी भी परिवर्तन के लिए सहमति, दस्तावेजीकरण और अनुमोदन आवश्यक है।

29.2 आपूर्तिकर्ता सेवाओं में परिवर्तन का प्रबंधन

आपूर्तिकर्ता की सेवाओं में महत्वपूर्ण परिवर्तनों की सूचना सूचना प्रणाली समिति को दी जाएगी। ये परिवर्तन इस प्रकार हैं:

- व्यवसाय प्रणाली और प्रक्रियाओं की गंभीरता को ध्यान में रखें।
- जोखिमों का पुनः मूल्यांकन किया जाना चाहिए।

आपूर्तिकर्ताओं के साथ अनुबंधों में परिवर्तनों की समीक्षा की जाएगी तथा नीति के अनुसार उन्हें अनुमोदित किया जाएगा।

30 परियोजना प्रबंधन

- हडको, संगठन द्वारा शुरू की गई आईटी परियोजनाओं के लिए एक सुसंगत और सुपरिभाषित परियोजना प्रबंधन दृष्टिकोण अपनाएगा। इस दृष्टिकोण में परियोजना जोखिमों और प्रगति की प्रभावी निगरानी और प्रबंधन सुनिश्चित करने के लिए शेयरधारकों की उचित भागीदारी शामिल होगी।
- नवीनतम या उभरती प्रौद्योगिकियों, उपकरणों को अपनाते समय, या मौजूदा प्रौद्योगिकी स्टैक को उन्नत करते समय, हडको एक मानकीकृत उद्यम वास्तुकला नियोजन पद्धति या ढांचे का पालन करेगा।
- नवीनतम या उभरती हुई तकनीकों को अपनाना हडको की समग्र व्यावसायिक/आईटी कौशलनीति और जोखिम क्षमता के अनुरूप होना चाहिए। इससे संगठन में सूचना के सुरक्षित और लचीले निर्माण, उपयोग या साझाकरण को बढ़ावा मिलना चाहिए।
- हडको अनुप्रयोगों और सूचना प्रणालियों में निर्बाध डेटा साझाकरण को सक्षम करने के लिए एक उद्यम डेटा शब्दकोश बनाए रखेगा, जिससे डेटा की सामान्य समझ को बढ़ावा मिलेगा।
- हडको यह सुनिश्चित करेगा कि सॉफ्टवेयर अनुप्रयोगों का सॉफ्टवेयर विक्रेताओं द्वारा पर्याप्त रूप से रखरखाव और समर्थन किया जाए, तथा इस आवश्यकता को लागू करने के लिए औपचारिक समझौते किए जाएं।
- हडको अपने विक्रेताओं से सभी महत्वपूर्ण अनुप्रयोगों के लिए स्रोत कोड प्राप्त करेगा। जहाँ स्रोत कोड प्राप्त करना संभव न हो, वहाँ हडको विक्रेता द्वारा चूक के जोखिम को पर्याप्त रूप से कम करने के लिए स्रोत कोड एस्क्रो व्यवस्था या अन्य व्यवस्थाएँ स्थापित करेगा। हडको यह सुनिश्चित करेगा कि सभी उत्पाद अद्यतन और कार्यक्रम सुधार स्रोत कोड एस्क्रो व्यवस्था में शामिल हों।
- हडको, एप्लिकेशन डेवलपर या विक्रेता से एक प्रमाणपत्र या लिखित पुष्टि प्राप्त करेगा जिसमें यह बताया जाएगा कि एप्लिकेशन ज्ञात कमियों, मैलवेयर और कोड में किसी भी गुप्त चैनल से मुक्त है। ऐसा प्रमाणपत्र या लिखित पुष्टि तब भी प्राप्त की जाएगी जब कोड में अपग्रेड सहित कोई भी महत्वपूर्ण परिवर्तन होगा।
- व्यवसाय उत्पाद के रूप में पेश किए जाने के लिए प्रस्तावित कोई भी नया आईटी अनुप्रयोग उत्पाद अनुमोदन के अधीन होगा।

31. डेटा माइग्रेशन नियंत्रण

इंटेलेक्ट के लाइव होने के बाद, व्यवसाय की निरंतरता बनाए रखने के लिए, पुराने सिस्टम से नए सिस्टम में सुचारू रूप से संक्रमण के लिए डेटा माइग्रेशन प्रक्रिया अनिवार्य है। माइग्रेशन प्रक्रिया, नए सिस्टम में माइग्रेट होने पर बिना किसी नुकसान के डेटा के स्थानांतरण को सुगम बनाएगी और साथ ही, माइग्रेशन से पहले और बाद में विभिन्न अखंडता जाँचों के माध्यम से माइग्रेट किए गए डेटा की अखंडता सुनिश्चित करेगी। माइग्रेशन, व्यवसाय को मौजूदा डेटा को साफ़ करने का विकल्प प्रदान करेगा।

हडको के पास एक प्रलेखित डेटा माइग्रेशन कौशलनीति होगी जिसमें डेटा माइग्रेशन की एक व्यवस्थित प्रक्रिया निर्दिष्ट की जाएगी, जिससे डेटा की अखंडता, पूर्णता और एकरूपता सुनिश्चित होगी। इस दस्तावेज़ में, अन्य बातों के साथ-साथ, माइग्रेशन के प्रत्येक चरण पर व्यावसायिक उपयोगकर्ताओं और एप्लिकेशन स्वामियों से अनुमोदन, ऑडिट ट्रेल्स के रखरखाव आदि से संबंधित प्रावधान शामिल होंगे।

- डेटा के अनधिकृत संशोधन को रोकने के लिए, हडको यह सुनिश्चित करेगा कि महत्वपूर्ण अनुप्रयोगों के संबंध में, डेटा को एक प्रक्रिया से दूसरी प्रक्रिया में या एक अनुप्रयोग से दूसरे अनुप्रयोग में स्थानांतरित करते समय डेटा में कोई मैनुअल हस्तक्षेप या मैनुअल संशोधन न हो।
- प्रक्रियाओं या अनुप्रयोगों के बीच डेटा स्थानांतरण प्रणाली का उचित रूप से परीक्षण किया जाना चाहिए, आवश्यक जांच और संतुलन के साथ सुरक्षित रूप से स्वचालित किया जाना चाहिए, और उचित प्रमाणीकरण प्रचलन और ऑडिट ट्रेल्स के साथ "सीधे प्रसंस्करण" पद्धति के माध्यम से उचित रूप से एकीकृत किया जाना चाहिए।

32. भेद्यता मूल्यांकन (वीए) / प्रवेश परीक्षण (पीटी) का संचालन

- महत्वपूर्ण सूचना प्रणालियों और/या विसैन्यीकृत क्षेत्र (डीएमजेड) में स्थित उन प्रणालियों के लिए, जिनके ग्राहक इंटरफ़ेस हैं, वीए (वैल्यूएशन) हर छह महीने में कम से कम एक बार और पीटी (प्रशिक्षण) हर 12 महीने में कम से कम एक बार आयोजित किया जाएगा। इसके अतिरिक्त, हडको ऐसी सूचना प्रणालियों के लिए उनके पूरे जीवनचक्र (कार्यान्वयन-पूर्व, कार्यान्वयन-पश्चात, बड़े बदलावों के बाद, आदि) के दौरान वीए/पीटी (प्रशिक्षण) आयोजित करेगा।
- गैर-महत्वपूर्ण सूचना प्रणालियों के लिए, वीए/पीटी के संचालन की आवश्यकता और आवधिकता निर्धारित करने के लिए जोखिम-आधारित दृष्टिकोण अपनाया जाएगा।
- वीए/पीटी का कार्य उचित रूप से प्रशिक्षित और स्वतंत्र सूचना सुरक्षा विशेषज्ञों/लेखा परीक्षकों द्वारा किया जाएगा।
- कार्यान्वयन के बाद के परिदृश्यों (जैसे, आईटी परियोजना/प्रणाली उन्नयन) में, वीए/पीटी उत्पादन परिवेश में आयोजित किया जाएगा। अपरिहार्य परिस्थितियों में, यदि पीटी परीक्षण परिवेश में आयोजित किया जाता है, तो हडको यह सुनिश्चित करेगा कि परीक्षण परिवेश का संस्करण और विन्यास उत्पादन परिवेश से काफी मिलता-जुलता हो। किसी भी विचलन का दस्तावेजीकरण और आईएससी द्वारा अनुमोदन किया जाना आवश्यक है।
- हडको यह सुनिश्चित करेगा कि पहचानी गई कमियों और संबंधित जोखिमों को आवश्यक सुधारात्मक उपायों को लागू करके तुरंत संबोधित किया जाए और ज्ञात कमियों की पुनरावृत्ति को रोकने के लिए निरंतर अनुपालन सुनिश्चित किया जाए, जैसे कि सामान्य कमियों और जोखिम (सीवीई) डेटाबेस में सूचीबद्ध हैं।

- हडको वीए/पीटी के संचालन के लिए एक प्रलेखित दृष्टिकोण स्थापित करेगा, जिसमें दायरा, कवरेज, भेद्यता स्कोरिंग प्रणाली (जैसे, कॉमन वल्नरेबिलिटी स्कोरिंग सिस्टम), और सभी संबंधित पहलुओं को शामिल किया जाएगा। यह दृष्टिकोण क्लाउड वातावरण में होस्ट की गई हडको की सूचना सिस्टम पर भी लागू होगा।

33. साइबर संकट प्रबंधन योजना

- साइबर संकट प्रबंधन योजना (सीसीएमपी) का उद्देश्य उन साइबर घटनाओं के लिए एक व्यवस्थित, समन्वित और प्रभावी प्रतिक्रिया सुनिश्चित करना है जो हडको के संचालन को बाधित कर सकती हैं, संवेदनशील डेटा से समझौता कर सकती हैं, या शेयरधारकों को प्रभावित कर सकती हैं। यह योजना ऐसी घटनाओं के प्रभाव को कम करने और सामान्य स्थिति में शीघ्र वापसी सुनिश्चित करने पर केंद्रित है।
- सूचना सुरक्षा नीति में, अन्य बातों के साथ-साथ, नीति के उद्देश्य, दायरा, स्वामित्व और उत्तरदायित्व; सूचना सुरक्षा संगठनात्मक संरचना; अपवाद; अनुपालन समीक्षा और नीतियों का अनुपालन न करने पर दंडात्मक उपायों जैसे पहलुओं पर विचार किया जाएगा। हडको एक साइबर सुरक्षा नीति और साइबर संकट प्रबंधन योजना (सीसीएमपी) भी तैयार करेगा।
- प्रभावी सीसीएमपी निम्नलिखित लक्ष्य को पूरा करेगा:
    - साइबर घटना और संकट संचार के प्रबंधन के लिए एक अनुकूलित कौशलनीति विकसित और कार्यान्वित करना
    - परिश्रमी संकट प्रबंधन और संचार के माध्यम से प्रतिष्ठा की रक्षा और वृद्धि करना
- साइबर संकट प्रबंधन योजना, व्यावसायिक व्यवधानों के प्रबंधन की क्षमता और तत्परता है ताकि सेवाओं की निरंतरता न्यूनतम स्वीकार्य स्तर पर बनी रहे और हडको की वित्तीय एवं प्रतिस्पर्धी स्थिति सुरक्षित रहे। सीसीएमपी निम्नलिखित चार पहलुओं पर ध्यान केंद्रित करता है: (i) पता लगाना (ii) प्रतिक्रिया (iii) पुनर्प्राप्ति और (iv) नियंत्रण। साइबर संकट प्रबंधन योजना में शामिल श्रेणियाँ हैं:
    - संकट प्रबंधन का संगठन
    - संकट प्रबंधन प्रक्रिया और जीवनचक्र
    - संकट प्रबंधन और संचार दिशानिर्देश
    - साइबर सुरक्षा खतरे
    - आरबीआई के साथ साइबर सुरक्षा घटनाओं पर जानकारी साझा करना
    - साइबर सुरक्षा घटना रिपोर्टिंग फॉर्म
    - डिजिटल साक्ष्य को संभालने के लिए दिशानिर्देश

34.1 सीसीएमपी का उद्देश्य

हडको को सामान्य व्यावसायिक संचालन को प्रभावित करने वाले साइबर संकट की स्थिति में साइबर संकट प्रबंधन योजना (सीसीएमपी) का उद्देश्य अपनी गतिविधियों को पुनः प्राप्त करने या बनाए रखने में सक्षम बनाना है। सीसीएमपी का उद्देश्य प्रमुख शेयरधारकों के प्रतिनिधित्व के साथ एक औपचारिक प्रतिक्रिया संरचना स्थापित करना है ताकि हडको को संकट का प्रभावी ढंग से जवाब देने में सहायता मिल सके और व्यावसायिक प्रभाव न्यूनतम हो जिससे अपेक्षित समयावधि के भीतर अपने प्रभावित सिस्टम की पुनर्प्राप्ति और बहाली सुनिश्चित हो सके।

प्रभावी सीसीएमपी निम्नलिखित लक्ष्य को पूरा करेगा:

- साइबर घटना और संकट संचार के प्रबंधन के लिए एक अनुकूलित कौशलनीति विकसित और कार्यान्वित करना।
- परिश्रमी संकट प्रबंधन और संचार के माध्यम से प्रतिष्ठा की रक्षा और वृद्धि करना

34.2 साइबर संकट प्रबंधन योजना का दायरा

साइबर संकट प्रबंधन योजना एक सुपरिभाषित और प्रलेखित कार्य योजना है, जिसके परिणामस्वरूप प्रतिकूल परिणाम सामने आते हैं जिसका उपयोग संकट के समय किया जा सकता है, जैसे कि सिस्टम की अनुपलब्धता/डाउनटाइम, जिसमें आमतौर पर प्रमुख कार्मिक, संसाधन, सेवाएं और परिणामी कार्य शामिल होते हैं।

34.3 संकट प्रबंधन टीम

साइबर संकट की स्थिति में निर्बाध समन्वय और निर्णय लेने के लिए हडको की संकट प्रबंधन टीम (सीएमटी) की स्थापना की गई है।

a) सीएमटी में निम्नलिखित अधिकारी शामिल होंगे:
b) अध्यक्ष एवं प्रबंध निदेशक (सीएमडी)
c) प्रमुख (आईटी)
d) मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ)
e) संकट से संबंधित विभागों के प्रमुख
f) सूचना सुरक्षा टीम के सदस्य

सूचना परिसंपत्तियों की उपलब्धता से संबंधित किसी भी संकट की स्थिति में, बीसीपी लागू की जाएगी। यदि संकट गोपनीयता और अखंडता को प्रभावित करता है, तो साइबर संकट प्रबंधन योजना (सीसीएमपी) लागू की जाएगी। सीसीएमपी लागू करते समय, जब भी व्यावसायिक निरंतरता स्थापित करने की आवश्यकता होगी, सीसीएमपी के अंतर्गत बीसीपी लागू की जाएगी।

संकट प्रबंधन टीम निम्नलिखित सुनिश्चित करेगी:

- हडको सुनिश्चित करें कि प्रासंगिक खतरा खुफिया फीड प्राप्त करता है (एसओसी के कार्यान्वयन के माध्यम से और सलाह/खतरा फीड के अनुपालन के लिए आवश्यक सुधारात्मक कार्रवाई पर वित्तीय संस्थान को सलाह देता है)।
- तैयार की गई संकट प्रबंधन योजना की प्रभावकारिता पर चर्चा करने के लिए समय-समय पर (कम से कम वार्षिक रूप से) बैठक करें।
- संकट की स्थिति और व्यवसाय पर उसके प्रभाव का विश्लेषण करें।
- .पहचानी गई घटना और घटना की गंभीरता का आकलन करने के आधार पर साइबर संकट प्रबंधन योजना लागू करने का निर्णय लें। सीएमटी संबंधित विभागाध्यक्षों के साथ समन्वय करेगा और प्रभावित विभागाध्यक्षों को सूचित करेगा।
- सीसीएमपी की सभी प्रक्रिया गतिविधियों का पालन करें।
- साइबर संकट से उबरने के लिए संबंधित शेयरधारकों को मार्गदर्शन प्रदान करना।
- संकट प्रबंधन के लिए पर्याप्त साक्ष्य संग्रह और जांच सुनिश्चित करना।

- पिछले संकट से सीखे गए सबक और परिणामस्वरूप साइबर सुरक्षा नियंत्रण, साइबर सुरक्षा नीति और साइबर संकट प्रबंधन योजना में सुधार पर चर्चा करें।
- साइबर संकट प्रबंधन योजना लागू होने पर संकट समाधान टीम का गठन करें। संकट से निपटने के लिए गतिविधियों को प्राथमिकता दें। यह साइबर संकट समाधान टीम घटना प्रतिक्रिया के लिए आवश्यक कौशलनीति और आगे बढ़ने में मदद करेगी।
- साइबर संकट उत्पन्न होने पर मूल कारण और वित्तीय संस्थान पर प्रभाव की जांच का दायरा निर्धारित करना।
- संकट की प्रकृति और गंभीरता के आधार पर विभिन्न नियामकों/सरकारीशासी निकायों/एजेंसियों जैसे कि सीईआरटी-इन, आरबीआई, पुलिस के साइबर अपराध सेल आदि के साथ समन्वय करना।
- ऐसे मामलों में बाह्य सहायता की व्यवस्था करें जहां आंतरिक संकट प्रबंधन टीम संकट को संभाल नहीं सकती।

34.3.1 संकट प्रबंधन प्रक्रिया

34.3.2 पता लगाना और प्रारंभिक रिपोर्टिंग

हडको परिवेश में किसी भी व्यक्ति द्वारा घटना की रिपोर्ट की जा सकती है; तथापि, आमतौर पर संसाधनों/सेवाओं के प्रबंधन और निगरानी में शामिल निम्नलिखित व्यक्तियों/समूहों में से किसी एक द्वारा इसकी रिपोर्ट की जाती है:

1. आईटी विभाग के अधिकारी
2. सुरक्षा संचालन केंद्र (एसओसी) टीम
3. नेटवर्क और सिस्टम सपोर्ट (एनएसएस) इंजीनियर
4. वेब/सिस्टम/नेटवर्क/डेटाबेस प्रशासक
5. प्रशासन (व्यक्तिगत सुरक्षा) टीम
6. सीआईएसओ
7. व्यवसाय इकाई का प्रमुख
8. ग्राहक और आपूर्तिकर्ता सहित अंतिम उपयोगकर्ता

सभी सुरक्षा घटनाएं या सुरक्षा नीतियों का उल्लंघन, जिनके बारे में अंतिम उपयोगकर्ता को जानकारी है, गवाह है या उसे सूचित किया गया है, उन्हें आईटी विभाग और सीआईएसओ को सूचित किया जाना चाहिए।

34.3.3 संकट को परिभाषित करना

सूचना और परिस्थितियों के विश्लेषण के बाद, सीआईएसओ आईटी विभागाध्यक्ष के परामर्श से घटना को साइबर संकट के रूप में वर्गीकृत करेगा।

34.3.4 संकट का आह्वान

- सीआईएसओ, आईटी विभागाध्यक्ष के परामर्श से, संकट की घोषणा करेगा और सीएमटी बैठक बुलाने का अनुरोध करेगा।

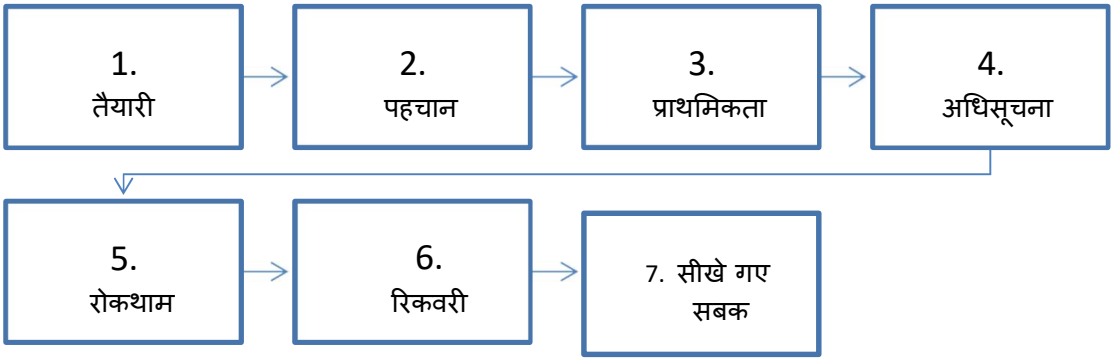
- सीएमटी साइबर संकट प्रबंधन योजना लागू करने के लिए संबंधित विभागों के साथ समन्वय करेगा।
- संकट समाधान टीम की ज़िम्मेदारी है कि सीएमटी संकट समाधान टीम को सूचित करेगा। वह शमन योजना को लागू करे और साइबर संकट का निवारण करे।

34.3.5 संकट समाधान और संकटोत्तर संचार

संकट समाधान टीम की ज़िम्मेदारी है कि वह शमन योजना को क्रियान्वित करे और साइबर संकट का निवारण करे। संकट के पूर्ण समाधान और व्यावसायिक संचालन की बहाली सुनिश्चित होने तक सीएमटी सक्रिय रहेगी। संकट समाधान के बाद, सीएमटी शेयरधारकों के बीच संकटोत्तर संचार को आगे बढ़ाएगी।

34.3.6 साइबर संकट प्रतिक्रिया पद्धति

साइबर संकट से निपटने के विभिन्न चरणों को नीचे चित्र में दर्शाया गया है-



34.3.7 तैयारी

हडको में तैयारी का चरण घटना से निपटने वाले कर्मियों के प्रशिक्षण, संसाधनों तक पहुँच और खतरे के प्रति जागरूकता पर केंद्रित होगा। घटना से निपटने की प्रक्रियाओं के अलावा, कुछ महत्वपूर्ण क्षेत्र हैं जिनमें वित्तीय संस्थान को अच्छी तरह प्रशिक्षित होना चाहिए, लेकिन केवल इन्हीं तक सीमित नहीं होना चाहिए:

- सिस्टम सख्त करना
- थ्रेट मॉडलिंग
- सिस्टम लॉग की ऑनलाइन निगरानी और विश्लेषण
- प्रवेश परीक्षण उपकरण और तकनीकें
- सूचना सुरक्षा नीति और साइबर सुरक्षा नीति के अनुसार फोरेंसिक तैयारी
- नेटवर्क डिवाइस और फ़ायरवॉल
- साइबर लचीलापन अभ्यास जैसे कि डीडीओएस सिमुलेशन परीक्षण, फ़िशिंग अभियान आदि।

- लचीलापन अभ्यास से सीख को संकट प्रबंधन योजना में साइबर शामिल करना
- साइबर संकट प्रबंधन योजना का आवधिक परीक्षण संकट की तैयारी के लिए निम्नलिखित दिशानिर्देशों का उपयोग किया जाएगा:

- वित्तीय संस्थान के भीतर एवं बाहरी टीम सदस्यों और अन्य लोगों (प्राथमिक और बैकअप संपर्क) की संपर्क जानकारी, जिसमें विधिक प्रवर्तन और अन्य संकट समाधान टीम शामिल हैं। जानकारी में फ़ोन नंबर, ईमेल पते और संपर्क की पहचान सत्यापित करने के निर्देश शामिल होंगे।
- संगठन के भीतर अन्य टीमों के लिए ऑन-कॉल जानकारी, जिसमें एस्केलेशन भी शामिल है।
- संकट रिपोर्टिंग प्रणाली, जैसे फोन नंबर, ईमेल पते, और/या ऑनलाइन फॉर्म जिनका उपयोग उपयोगकर्ता संदिग्ध घटनाओं की रिपोर्ट करने के लिए कर सकते हैं।
- टीम के सदस्यों को ऑफ-ऑवर सहायता और ऑन-साइट संचार के लिए मोबाइल फोन साथ रखना होगा।
- केंद्रीय संचार और समन्वय के लिए "वॉर रूम": यदि स्थायी वॉर रूम आवश्यक या व्यावहारिक नहीं है, तो टीम को संकट प्रबंधन के लिए एक आभासी वातावरण बनाने की प्रक्रिया बनानी चाहिए।

34.3.8 घटनाओं के लिए ट्रिगर:

- प्रणालियों, नेटवर्कों और प्रक्रियाओं के कामकाज में कुछ लक्षणों और विसंगतियों का अवलोकन।
- वित्तीय संस्थान के सुरक्षा उपकरणों जैसे सुरक्षा घटना और घटना प्रबंधन (SIEM) पर अलर्ट देखे गए।
- किसी प्रणाली का संक्रमण, आक्रमण या घुसपैठ या खराबी या सूचना परिसंपत्तियों/प्रणालियों को नुकसान की सूचना
- सीईआरटी-इन और अन्य नियामक टीमों/सुरक्षा एजेंसियों जैसे बाहरी संगठनों से अलर्ट प्राप्त होते हैं।

34.3.9 घटनाओं के लक्षण और प्रतिक्रिया कार्रवाई:

सभी प्रकार के उपयोगकर्ताओं द्वारा देखी जाने वाली घटना के सामान्य लक्षण, पता लगाने का स्रोत, अपेक्षित प्रतिक्रिया कार्रवाई और कार्रवाई के लिए जिम्मेदार व्यक्ति।

इस चरण के एक भाग के रूप में निम्नलिखित गतिविधियाँ की जानी चाहिए:

1. सुनिश्चित करें कि सभी गतिविधियां, परिणाम और लिए गए निर्णय भविष्य के विश्लेषण के लिए लॉग किए गए हैं।
2. सुनिश्चित करें कि साक्ष्य एकत्रित किए जाएं, सुरक्षित रूप से संग्रहीत किए जाएं तथा उनकी निरंतर निगरानी की जाए।
3. यह समझने के लिए विश्लेषण करें कि क्या यह घटना एक संभावित साइबर सुरक्षा घटना है या एक गलत अलार्म है।
4. यदि यह पुष्टि हो जाती है कि यह साइबर सुरक्षा घटना है, तो घटना को घटना वर्गीकरण मानदंडों के अनुसार वर्गीकृत करें, परिणाम सीएमटी को बताएं।

5. सीएमटी को रिपोर्ट की गई घटनाओं और संकट के लिए पूर्व-निर्धारित मानदंडों के आधार पर, सीएमटी घटना को संकट के रूप में वर्गीकृत करेगा और संकट प्रबंधन योजना लागू करेगा।
6. संकट की स्थिति में, सीएमटी एक प्रारंभिक संकट रेटिंग भी प्रदान करेगा जो संकट के दौरान बदल भी सकती है।
7. सीएमटी संकट स्टॉक चरण के दौरान अपने निजी पोर्टफोलियो का निजीकरण।
8. सीएमटी निम्नलिखित प्रमुख गतिविधियों की व्यवस्था करेगा:

    - सिस्टम/नेटवर्क विसंगतियों और घटनाओं का विश्लेषण करें
    - उपलब्ध डेटा/अलर्ट के आधार पर घटना का विश्लेषण करें
    - घटना का विस्तृत विश्लेषण करने के लिए बाद के चरणों में कम से कम 3 महीने तक स्थानीय लॉग, सिस्टलॉग, सक्रिय निर्देशिका जैसे लॉग स्रोतों और फायरवॉल, आईडीएस/आईपीएस आदि जैसे सुरक्षा उपकरणों से अलर्ट से प्रभावित सिस्टम से लॉग पुनर्प्राप्त करें।
    - आगे की जाँच और विधिक कार्रवाई में साक्ष्य के रूप में कच्चे लॉग आवश्यक हैं। लॉग की पुनर्प्राप्ति और उनका सुरक्षित रखरखाव संकट से निपटने वाली टीमों की प्राथमिकता होनी चाहिए।
    - घटना से कम से कम 24 घंटे पहले लॉग का विश्लेषण किया जाएगा।
    - यह विश्लेषण संकट घोषित होने के 60 मिनट के भीतर सीएमटी को वापस भेजना होगा। विश्लेषण में संकट को नियंत्रित करने के संभावित उपाय भी शामिल होने चाहिए। (ध्यान दें कि आरबीआई ने प्रारंभिक घटना रिपोर्टिंग के लिए दो से छह घंटे का समय दिया है)।
    - यदि उपर्युक्त समय के भीतर कोई संदिग्ध घटना नहीं पाई जाती है, तो व्यापक समय सीमा के लिए विश्लेषण किया जाना चाहिए।

34.3.10 अधिसूचना

आंतरिक शेयरधारक अधिसूचनाएँ:

आईटी विभागाध्यक्ष और सीआईएसओ, जो पुनर्प्राप्ति प्रक्रियाओं में सक्रिय रूप से भाग लेंगे, उन्हें टेलीफोन पर सूचित किया जाएगा। अन्य अंतिम उपयोगकर्ता, यदि प्रभावित होते हैं, तो उन्हें सीधे मेल द्वारा या संबंधित विभागाध्यक्षों (जिन्हें टेलीफोन पर सूचित किया जाएगा) के माध्यम से सूचित किया जाएगा। संचार में प्रभावित सेवाओं (एप्लिकेशन, वेब पोर्टल, ईमेल सेवा या समग्र नेटवर्क कनेक्टिविटी), व्यवधान का कारण और संचालन पुनः आरंभ करने में लगने वाले अनुमानित समय का विवरण शामिल होगा।

बाहरी शेयरधारकों की अधिसूचनाएँ:

- नेतृत्व टीम को स्थिति के बारे में जानकारी दी जाएगी।
- कंपनी के प्रवक्ता की पहचान की जाएगी और उन्हें स्थिति से अवगत कराया जाएगा।
- कंपनी का विवरण यदि आवश्यक हो तो तैयार किया जाएगा और मीडिया तथा अन्य संगठनों को जारी किया जाएगा।
- यदि आवश्यक हुआ तो मीडिया कवरेज प्रसारण का आयोजन और सुविधा प्रदान की जाएगी।
- आपातकाल से जुड़ी बदलती घटनाओं को लगातार अनुकूलित किया जाएगा।

यदि ऐसा संकट बाह्य संस्थाओं पर प्रतिकूल प्रभाव डालता है, तो नियामक निकायों अर्थात सीईआरटी-इन/आरबीआई, एनसीआईआईपीसी आदि को प्रारंभिक घटना का पता चलने के बाद निर्धारित समय के भीतर संकट के बारे में विधिवत सूचित किया जाएगा।

34.3.11 नियंत्रण

संकट से निपटने के लिए दो प्रमुख नियंत्रण कौशलनीतियाँ उपयोग में लाई जा सकती हैं:

तत्काल नियंत्रण:

यह मैलवेयर और दुर्भावनापूर्ण ट्रैफ़िक उत्पन्न करने वाले होस्ट्स के लिए एक मानक प्रक्रिया है। इस परिदृश्य में होस्ट (या होस्ट्स) को नेटवर्क से हटा दिया जाता है/अलग कर दिया जाता है।

1. इस परिदृश्य में, स्रोत और प्रभावित दोनों प्रणालियों को वित्तीय संस्थान के नेटवर्क से अलग करना होगा।
2. अलगाव निम्नलिखित में से एक या अधिक द्वारा किया जा सकता है:
   - प्रभावित सिस्टम के नेटवर्क कनेक्शन को भौतिक रूप से डिस्कनेक्ट करना
   - प्रभावित सिस्टम या नेटवर्क सेगमेंट को तार्किक रूप से अलग करना। इन परिदृश्यों में इंटरनेट, अन्य महत्वपूर्ण सेगमेंट, उपयोगकर्ता सेगमेंट आदि से अलग करना शामिल हो सकता है।
   - उपयोगकर्ता का लॉगिन अक्षम करना ।
3. पृथक करने का निर्णय समझौता, व्यवसाय निरंतरता प्रक्रियाओं, आपदा पुनर्प्राप्ति योजना की पर्याप्तता की प्रारंभिक समझ के आधार पर लिया जाना चाहिए।
4. यदि प्रणालियों को अलग करना एक चुनौती है या अलग करने की आवश्यकता महसूस नहीं की जाती है, तो संकट से कम से कम 24 घंटे पहले या संकट के मूल कारण का पता लगने तक सभी व्यावसायिक और गैर-व्यावसायिक लेनदेन का विश्लेषण व्यावसायिक टीमों द्वारा किया जाना चाहिए।
5. सीएमटी को व्यवसाय संचालन को सुचारू रूप से चलाने के लिए यदि आवश्यक हो, तो डीआर साइट पर स्विचओवर सुनिश्चित करने हेतु बीसीपी संकट को लागू करने का निर्णय लेना चाहिए।

विलंबित नियंत्रण:

- घटना को रोकने से पहले, सक्रिय अपराधियों पर नज़र रखकर अतिरिक्त सबूत इकट्ठा करने की कोशिश कौशलनीति का इस्तेमाल संकट समाधान टीम द्वारा किया जाता हैं। यह एक उन्नत कौशलनीति है जो अत्यंत गंभीर परिस्थितियों के अलावा लागू नहीं होगी। हालाँकि, किसी महत्वपूर्ण उत्पादन मशीन के मामले में, उसे नियंत्रण के लिए तुरंत नेटवर्क से हटाना संभव नहीं हो सकता है।
- इस कौशलनीति का उपयोग संकट समाधान टीमों द्वारा किया जाता है जो घटना को रोकने से पहले लाइव पैटर्न का अवलोकन करके अतिरिक्त साक्ष्य इकट्ठा करने की कोशिश कर रहे हैं।
- यह एक उन्नत कौशलनीति है जो तब तक लागू नहीं होगी जब तक कि कोई अत्यंत गंभीर परिस्थिति न हो या जब लेन-देन या संदेशों के आगे के प्रसारण को रोका न जा सके।
- विलंबित नियंत्रण कौशलनीति का सावधानीपूर्वक पालन किया जाना चाहिए, क्योंकि हमलावर अनधिकृत एक्सेस को बढ़ा सकता है या अन्य प्रणालियों को प्रभावित कर सकता है। विलंबित नियंत्रण में भी, प्रारंभिक नियंत्रण का एक निश्चित स्तर होना चाहिए, जैसे प्रभावित खंड को अलग करना लेकिन प्रभावित प्रणालियों के नियंत्रण में देरी करना।

- नियंत्रण कौशलनीतियों का निर्णय व्यवसाय प्रभाव के आधार पर किया जाएगा।

34.3.12 रिकवरी

घटना के संकट में बदलने पर, विभाग तुरंत अपनी आकस्मिक योजनाओं को लागू करेंगे। यदि स्थिति व्यापक है और वित्तीय संस्थान स्तर पर प्रतिक्रिया की आवश्यकता है, तो सीएमटी के परामर्श से प्रतिक्रिया कार्रवाई शुरू की जाएगी। सीएमटी द्वारा वॉर रूम को सक्रिय किया जाएगा।

प्रतिक्रिया योजना में विभिन्न प्रकार के साइबर संकटों के संकेतों को रेखांकित किया गया है, जो आम तौर पर उपयोगकर्ताओं, सिस्टम प्रशासकों और उपकरण-आधारित पहचान प्रणालियों और प्रतिक्रिया कार्यों द्वारा देखे जा सकते हैं।

संकट को कम करने के लिए आवश्यक कदम प्रकृति और गंभीरता के अनुसार अलग-अलग होंगे।

34.3.13 सीखे गए पाठ

संकट से सफलतापूर्वक निपटने और उबरने के बाद, भविष्य में संदर्भ/सावधानी के लिए (घटना को बंद करने से पहले) निम्नलिखित कार्य किए जाने आवश्यक हैं:

1. संकट के बाद का विश्लेषण करें तथा संगठन और विभाग स्तर पर अपनाई गई संकट प्रतिक्रिया का भी विश्लेषण करें।
2. उन्मूलन प्रणाली को बेहतर बनाने और अनुकूलित करने के लिए तकनीकी दृष्टिकोण से हमले का मूल्यांकन और आकलन करना।
3. संकट से सीखे गए सबक को दस्तावेजित करें और संकट रिपोर्ट तैयार करें, जिसमें संकट के बाद बुनियादी ढांचे की सुरक्षा में सुधार शामिल हो।
4. सीखे गए पाठ के एक भाग के रूप में निम्नलिखित गतिविधियाँ की जानी चाहिए:
    - एक सबक दस्तावेज तैयार करें जिसमें प्रभावित प्रणाली का विवरण हो, एक्सेस कैसे प्राप्त की गई, कितना नुकसान हुआ तथा यदि साइबर संकट प्रबंधन योजना लागू नहीं की गई तो संभावित नुकसान क्या होगा।
    - पिछले हमलों के रुझान/पैटर्न की पहचान करें
    - गंभीर क्षेत्रों की पहचान करें
    - विश्लेषण करें कि भविष्य में ऐसे संकट की संभावना को कम करने के लिए क्या निवारक कार्रवाई की जा सकती है
    - कार्यान्वित सूचना और साइबर सुरक्षा नियंत्रणों की पहचान करना और उनमें सुधार करना
    - सूचना और साइबर सुरक्षा जोखिम मूल्यांकन ढांचे की पहचान और सुधार करना
    - सुरक्षा घटना/घटना/भेद्यता डेटाबेस को अद्यतन करें

5. संकट के निवारण की पुष्टि दर्ज की जाएगी और संकटोत्तर गतिविधि के भाग के रूप में भेजी जाएगी। विभागाध्यक्षों द्वारा विस्तृत मूल कारण विश्लेषण (आरसीए) तैयार किया जाएगा।

6. आईटी विभाग, सीआईएसओ कार्यालय के परामर्श से, भविष्य में ऐसी किसी भी आपदा से बचाव हेतु अवसंरचना संरचना को सुदृढ़ करने के उपाय लागू करेगा। इस उद्देश्य के लिए लागू/संवर्धित किए जाने वाले किसी भी भौतिक और पर्यावरणीय सुरक्षा नियंत्रण की ज़िम्मेदारी सुविधा/भवन प्रबंधन विभाग की होगी।

7. आवश्यकतानुसार घटना रिपोर्ट CERT-In, RBI आदि के साथ साझा करें। यह कार्य सीआईएसओ द्वारा किया जाएगा।

34. साइबर हमले का जीवन चक्र

साइबर हमले के जीवनचक्र के चरणों को नीचे दर्शाया गया है:

चरण-1: खुफिया जानकारी एकत्र करना या टोह लेना:

साइबर हमले के इस दौर में, अपराधी, साइबर अपराधी या हैकर अपने शिकार का ध्यानपूर्वक अध्ययन करते हैं और अपने हमलों की योजना बनाते हैं, अक्सर सोशल इंजीनियरिंग, फ़िशिंग, ईमेल एड्रेस हार्वेस्टिंग और अन्य हथकंडों का इस्तेमाल करके अपने लक्ष्यों की खोज, पहचान और चयन करते हैं। वे नेटवर्क की कमज़ोरियों, सेवाओं और शोषण की जा सकने वाली ऐप्लिकेशन की जाँच के लिए विभिन्न उपकरणों का भी इस्तेमाल करते हैं।

चरण 2: प्रारंभिक उपयोग :

हमलावर मैलवेयर पेलोड और उसे पहुँचाने के लिए इस्तेमाल की जाने वाली विधि निर्धारित करता है। उदाहरण के लिए, डेटा फ़ाइलों या वेब पेजों को ऐसे एक्सप्लॉइट से हथियार बनाया जा सकता है जिनका इस्तेमाल पीड़ित के कमज़ोर सॉफ़्टवेयर को निशाना बनाने के लिए किया जाता है और उन्हें ईमेल अटैचमेंट या ड्राइव-बाय डाउनलोड के ज़रिए पहुँचाया जाता है। ड्राइव-बाय डाउनलोड, उपयोगकर्ता की जानकारी के बिना, आमतौर पर किसी ऑपरेटिंग सिस्टम, वेब ब्राउज़र या अन्य तृतीय-पक्ष एप्लिकेशन की कमज़ोरी का फ़ायदा उठाकर, पृष्ठभूमि में उन्नत मैलवेयर या एक्सप्लॉइट पहुँचाता है। हमलावर के पास आमतौर पर एक्सप्लॉइट करने के दो विकल्प होते हैं:

- सोशल इंजीनियरिंग एक अपेक्षाकृत सरल तकनीक है जिसका उपयोग किसी को दुर्भावनापूर्ण लिंक पर क्लिक करने या दुर्भावनापूर्ण निष्पादन योग्य फ़ाइल खोलने के लिए लुभाने के लिए किया जाता है।
- सॉफ़्टवेयर एक्सप्लॉइट एक परिष्कृत तकनीक है क्योंकि यह मूलतः ऑपरेटिंग सिस्टम, वेब ब्राउज़र, या अन्य तृतीय-पक्ष सॉफ़्टवेयर को हमलावर के कोड को चलाने के लिए प्रेरित करती है। इसका अर्थ है कि हमलावर को एंडपॉइंट पर विशिष्ट असुरक्षित सॉफ़्टवेयर को लक्षित करने के लिए एक एक्सप्लॉइट तैयार करना होता है। एक बार एक्सप्लॉइट सफल हो जाने पर, एक उन्नत मैलवेयर पेलोड स्थापित किया जा सकता है।

Step-3: चरण-3: कमांड और नियंत्रण (सीएनसी):

संचार एक सफल हमले का जीवनचक्र है। हमलावरों को कमांड और नियंत्रण प्राप्त करने और लक्ष्य सिस्टम या नेटवर्क से चुराए गए डेटा को निकालने के लिए संक्रमित सिस्टम के साथ संचार करने में सक्षम होना चाहिए। इस संचार का उपयोग हमलावर द्वारा पीड़ित के नेटवर्क पर अन्य सिस्टम को लक्षित करते हुए, पार्श्विक रूप से आगे बढ़ने के लिए भी किया जा सकता है। इस प्रकार, प्रारंभिक रूप से संक्रमित लक्ष्य केवल पहला प्रवेश बिंदु हो सकता है जो हमलावर के अंतिम लक्ष्य की ओर पार्श्विक गति को सक्षम बनाता है।

सीएनसी संचार आमतौर पर गुप्त होते हैं और नेटवर्क पर कोई संदेह पैदा नहीं कर सकते। इस तरह के ट्रैफ़िक को आमतौर पर निम्नलिखित तकनीकों के ज़रिए छिपाया या छिपाया जाता है:

- एसएसएल, एसएसएच या किसी अन्य कस्टम अनुप्रयोग के साथ एन्क्रिप्शन।
- प्रॉक्सी, रिमोट डेस्कटॉप एक्सेस टूल, या अन्य (अनुमत) अनुप्रयोगों या प्रोटोकॉल के भीतर अनुप्रयोगों को टनल करके परिहार।
- खुले या गैर-मानक बंदरगाहों पर सुरंग बनाने के लिए पोर्ट चोरी पोर्ट होपिंग का उपयोग करके ।
- फास्ट फ्लक्स (या डायनामिक डीएनएस) एकाधिक संक्रमित होस्टों के माध्यम से प्रॉक्सी करने, ट्रैफ़िक को पुनः रूट करने, तथा फोरेंसिक टीमों के लिए यह पता लगाना अत्यंत कठिन बना देता है कि ट्रैफ़िक वास्तव में कहां जा रहा है।

चरण-4: निजीकरण वृद्धि:

एक बार लक्ष्य एंडपॉइंट में घुसने के बाद, हमलावर को दृढ़ता (लचीलापन या उत्तरजीविता) सुनिश्चित करनी होती है। इस उद्देश्य के लिए विभिन्न प्रकार के उन्नत मैलवेयर का उपयोग किया जाता है, जिनमें निम्नलिखित शामिल हैं:

- रूटकिट्स मैलवेयर जो कंप्यूटर तक विशेषाधिकार प्राप्त (रूट-स्तर) एक्सेस प्रदान करते हैं।
- बूट किट रूटकिट्स के कर्नेल-मोड संस्करण हैं, जिनका उपयोग आमतौर पर उन कंप्यूटरों पर हमला करने के लिए किया जाता है जो पूर्ण डिस्क एन्क्रिप्शन द्वारा सुरक्षित होते हैं।
- बैकडोर हमलावर को सामान्य प्रमाणीकरण प्रक्रियाओं को बायपास कर किसी प्रभावित सिस्टम तक एक्सेस प्राप्त करने में सक्षम बनाता है और इन्हें अक्सर फेलओवर के रूप में स्थापित किया जाता है, ताकि अन्य मैलवेयर का पता लगने और सिस्टम से हटाए जाने की स्थिति में उन्हें रोका जा सके।
- संक्रमित एंडपॉइंट पर किसी भी वैध रूप से इंस्टॉल किए गए एंटीवायरस सॉफ़्टवेयर को निष्क्रिय करने के लिए एंटी-एवी सॉफ़्टवेयर भी इंस्टॉल किया जा सकता है, जिससे हमलावर द्वारा बाद में इंस्टॉल किए गए मैलवेयर का स्वतः पता लगाने और हटाने से रोका जा सकता है। कई एंटी-एवी प्रोग्राम किसी लक्षित एंडपॉइंट के मास्टर बूट रिकॉर्ड (एमबीआर) को संक्रमित करके काम करते हैं।

चरण-5: डेटा एक्सफ़िलट्रेशन

हमलावरों के हमले और डेटा चोरी के कई अलग-अलग मकसद होते हैं, जिनमें डेटा चोरी, महत्वपूर्ण बुनियादी ढाँचे का विनाश, हैकटिविज़्म या साइबर आतंकवाद शामिल हैं। हमले का यह अंतिम चरण अक्सर महीनों या सालों तक चलता है, खासकर जब उद्देश्य डेटा चोरी हो, क्योंकि हमलावर पता लगाने से बचने के लिए धीमी और धीमी हमले की रणनीति अपनाता है।

थ्रेट्स खतरों के प्रकार

थ्रेट्स	हमले का संभावित कारण
जटिल हमलावर	इस खतरे का संभावित कारण बैंक का इंटरनेट पर मौजूद होना और उसमें भेद्यता होना है।

जटिल हमलावर	इस तरह के खतरे का संभावित कारण यह है कि वित्तीय संस्थान इंटरनेट पर मौजूद है और उसके पास मूल्यवान जानकारी है।
थ्रेट्	हमले का संभावित कारण
निगम से संबन्धित जासूसी	इस तरह के खतरे का संभावित कारण गलत तरीकों से व्यापार रहस्यों तक एक्सेस प्राप्त करने का प्रयास है
संगठित अपराध	इस तरह के खतरे का संभावित कारण वित्तीय लाभ प्राप्त करना है
राज्य प्रायोजित हमले और उन्नत सतत खतरा	इस तरह के खतरे का संभावित कारण बैंक द्वारा किए जाने वाले कार्य का प्रकार और उसकी बौद्धिक संपदा का मूल्य है

34.1 साइबर हमले की रोकथाम कौशलनीतियाँ

साइबर लचीलेपन को हडको की साइबर हमलों का पूर्वानुमान लगाने, उनका सामना करने, तथा साइबर हमलों के कारण होने वाले किसी भी विघटनकारी प्रभाव को रोकने, तेज़ी से उबरने और बेहतर क्षमताओं तक विकसित होने की क्षमता के रूप में परिभाषित किया गया है। साइबर हमलों का सामना करने के लिए अपनाए जाने वाले तरीके निम्नलिखित हैं:

साइबर हमलों का सामना करने की तैयारी का परीक्षण

आईटी विभाग, सीआईएसओ के समन्वय से, अभ्यासों में भाग लेगा। ये अभ्यास और परीक्षण निर्धारित अंतराल पर आयोजित किए जाएँगे।

34.2 साइबर सुरक्षा तैयारी संकेतक

साइबर लचीलेपन ढाँचे की पर्याप्तता और उसके अनुपालन का आकलन और मापन जोखिम/तैयारी के स्तर का आकलन करने के लिए संकेतकों के विकास के माध्यम से किया जाता है। इन संकेतकों का उपयोग योग्य और सक्षम प्रोफेशनल द्वारा किए गए स्वतंत्र अनुपालन जाँच और ऑडिट के माध्यम से व्यापक परीक्षण के लिए किया जाएगा। इसका उद्देश्य नियंत्रणों की पहचान करना, प्रभावशीलता का आकलन करना, चिंता के क्षेत्रों की पहचान करना और फिर (साइबर सुरक्षा के दृष्टिकोण से) कमियों को दूर करने के लिए एक योजना तैयार करना है। कर्मचारियों सहित शेयरधारकों के बीच जागरूकता भी इस मूल्यांकन का एक हिस्सा हो सकती है।

34.3 सुरक्षा संचालन केंद्र (एसओसी)

इसका उद्देश्य जल्द से जल्द एसओसी की स्थापना करना है। एसओसी निरंतर निगरानी को सक्षम बनाएगा और लगातार बदलते खतरों से निपटने में सक्षम होगा। सक्रिय निगरानी और प्रबंधन क्षमताएँ एसओसी की प्रमुख विशेषताएँ होंगी। त्वरित पहचान और त्वरित प्रतिक्रिया प्रमुख कारक हैं जो साइबर सुरक्षा के प्रशासनिक पहलू को मज़बूत करेंगे। इसे प्राप्त करने के लिए, एसओसी के प्रमुख प्रवर्तक निम्नलिखित हैं:

- सुरक्षा घटनाओं की निगरानी, विश्लेषण और उन्हें आगे बढ़ाना
- प्रतिक्रिया विकसित करें - सुरक्षा करें, पता लगाएं, प्रतिक्रिया दें, पुनर्प्राप्त करें
- घटना प्रबंधन और फोरेंसिक विश्लेषण का संचालन करना

- वित्तीय संस्थान/बाहरी एजेंसियों के भीतर प्रासंगिक शेयरधारकों के साथ समन्वय

  हडको यह सुनिश्चित करेगा कि हडको का एसओसी एकीकृत हो, संचालित हो और 24*7 निगरानी में हो, तथा सुरक्षा सूचना और घटना प्रबंधन (एसआईईएम), खतरा खुफिया प्लेटफॉर्म (टीआईपी) जैसे उपकरणों से सुसज्जित हो, तथा अन्य सभी उपकरण जो दायरे और सेवा स्तरों के अनुपालन के लिए आवश्यक हैं।

35. सुरक्षित क्लाउड सेवाएँ

- सेवाएँ सुरक्षा और अनुपालन के लिए एक साझा ज़िम्मेदारी मॉडल का पालन करती हैं। इन मॉडलों की गहन जाँच करने और क्लाउड सेवाओं पर होस्ट किए गए परीक्षण, स्टेजिंग और बैकअप वातावरण के लिए उपयुक्त सुरक्षा नीतियों और उपायों को लागू करने की सलाह दी जाती है।
- उपयोग में आने वाले सभी क्लाउड इंस्टेंस की सार्वजनिक पहुँच की जाँच करें। सुनिश्चित करें कि कोई भी सर्वर/स्टोरेज अनुचित कॉन्फ़िगरेशन के कारण अनजाने में डेटा लीक न कर रहा हो।
- क्लाउड संसाधनों तक विस्तृत अनुमति के साथ एक्सेस नियंत्रण के लिए न्यूनतम विशेषाधिकार सिद्धांत को लागू करना।
- महत्वपूर्ण क्लाउड संसाधनों के लिए लॉगिंग के साथ-साथ क्लाउड नेटिव सुरक्षा नियंत्रण सक्षम करें और निरंतर निगरानी सुनिश्चित करें।
- सुनिश्चित करें कि उपयोगकर्ता अकाउंटखातों में बहु-कारक प्रमाणीकरण (एमएफए) हो, मजबूत पासवर्ड नीति हो, साथ ही जब कोई प्रशासक/उपयोगकर्ता संगठन छोड़ता है तो खाते को अक्षम करने की प्रक्रिया/मानक भी हो।
- हडको को क्लाउड सेवा मॉडल और प्राप्त सेवाओं का स्पष्ट दस्तावेजीकरण करना चाहिए।
- हडको को एक सुपरिभाषित क्लाउड सुरक्षा ढांचा स्थापित करना चाहिए जिसमें निम्नलिखित सुरक्षा परतें शामिल हों:
  - भौतिक और तार्किक सुरक्षा
  - आईटी इन्फ्रास्ट्रक्चर सुरक्षा
  - एप्लीकेशन और प्रक्रिया सुरक्षा
  - डेटा और सूचना सुरक्षा
  - क्लाउड सुरक्षा प्रबंधन
- पहचान और एक्सेस प्रबंधन: हडको को क्लाउड सेवा प्रदाता के परिसर में होस्ट किए गए डेटा तक एक्सेस हेतु नियंत्रण निर्धारित करने चाहिए। इसमें विशेषाधिकार प्राप्त प्रशासकों की नियुक्ति और निगरानी के बारे में विशिष्ट जानकारी प्राप्त करना और उनकी एक्सेस पर मज़बूत नियंत्रण स्थापित करना शामिल है।
- प्रमाणीकरण और प्राधिकरण: सभी प्रमाणीकरण आवश्यकताओं के लिए हडको की पासवर्ड नीति का पालन किया जाना चाहिए। आवश्यकता पड़ने पर भूमिका-आधारित प्रमाणीकरण लागू किया जाना चाहिए, और बहु-टेनन्ट वातावरण में अलग-अलग पहचान बनाए रखी जानी चाहिए।
- डेटा रेजीडेंसी: क्लाउड सेवा प्रदाता को यह सुनिश्चित करना होगा कि हडको का डेटा विशेष रूप से भारत के डेटा केंद्रों में ही रहे। सभी प्रसंस्करण भारत में ही किए जाने चाहिए, और बैकअप सहित कोई भी डेटा भारत के विधिक अधिकार क्षेत्र से बाहर प्रेषित नहीं किया जाना चाहिए।
- डेटा पृथक्करण: हडको को बहु- टेनन्ट क्लाउड वातावरण में डेटा पृथक्करण के लिए मजबूत नियंत्रण परिभाषित करना चाहिए।

- डेटा सुरक्षा: सभी सिस्टम इंटरफेस और व्यावसायिक कार्यों में हडको के डेटा की गोपनीयता, अखंडता और उपलब्धता सुनिश्चित करने के लिए नीतियाँ और प्रक्रियाएँ स्थापित और अनुरक्षित की जानी चाहिए। अनधिकृत प्रकटीकरण, परिवर्तन या विनाश को रोकने के लिए, स्थिर और पारगमन में डेटा के लिए मज़बूत एन्क्रिप्शन प्रणाली का उपयोग किया जाना चाहिए।
- हुडको को डेटा लॉगिंग, निगरानी और ऑडिटिंग के लिए स्पष्ट नियंत्रण स्थापित करना चाहिए।
- संभावित खतरों की पहचान करने और उन्हें दूर करने के लिए जोखिम-आधारित भेद्यता आकलन और प्रवेश परीक्षण नियमित रूप से किए जाने चाहिए।
- सेवा वितरण के डिज़ाइन और विकास के दौरान हडको और क्लाउड प्रदाता के बीच एक सहयोगात्मक शासन संरचना और प्रक्रियाएँ परिभाषित की जानी चाहिए। इन प्रक्रियाओं में सेवा जोखिम मूल्यांकन और प्रबंधन प्रोटोकॉल शामिल होने चाहिए और इन्हें सेवा समझौतों में शामिल किया जाना चाहिए।
- हडको को क्लाउड-आधारित समाधानों के लिए प्रभावी व्यवसाय निरंतरता और आपदा रिकवरी उपाय सुनिश्चित करना चाहिए।

36. एन्क्रिप्शन नीति

इस एन्क्रिप्शन नीति का उद्देश्य हडको में संवेदनशील डेटा के एन्क्रिप्शन के लिए दिशानिर्देश और सर्वोत्तम अभ्यास स्थापित करना है, जिससे पारगमन और स्थिर डेटा की गोपनीयता, अखंडता और उपलब्धता सुनिश्चित हो सके। यह नीति नेटवर्क पर संचरण के दौरान और क्लाउड स्टोरेज वॉल्यूम, डेटाबेस और फ़ाइल स्टोरेज सहित विभिन्न स्टोरेज घटकों में संग्रहीत होने पर डेटा को एन्क्रिप्ट करने की आवश्यकताओं को रेखांकित और एपीआई के माध्यम से संचरण भी करती है। साथ ही, इस नीति का उद्देश्य हडको और उसके ग्राहकों के डेटा को अनधिकृत पहुँच, अवरोधन और छेड़छाड़ से बचाना है, जिससे डेटा उल्लंघनों के जोखिम को कम किया जा सके और डेटा सुरक्षा का उच्च स्तर बनाए रखा जा सके।

- जब सूचना को सूचना प्रणालियों, मीडिया/उपकरणों में संग्रहीत किया जाता है या नेटवर्क पर एक्सेस/प्रेषित किया जाता है, तो उचित एन्क्रिप्शन तकनीकों के माध्यम से गुप्त/गोपनीय जानकारी की गोपनीयता, अखंडता, प्रामाणिकता और गैर-अस्वीकृति बनाए रखी जाएगी।
- हडको निम्नलिखित के लिए उपयुक्त एन्क्रिप्शन प्रणाली स्थापित करेगा: -
    - ट्रांजिट में डेटा: वह डेटा जो दो संचार पक्षों के बीच नेटवर्क पर प्रेषित किया जा रहा है, जैसे कि एपीआई, वेब एप्लिकेशन और अन्य संचार चैनलों के माध्यम से भेजा और प्राप्त किया गया डेटा।
    - डेटा एट रेस्ट: वह डेटा जो स्टोरेज सिस्टम, डेटाबेस या अन्य स्टोरेज मीडिया पर, चाहे वह ऑन-प्रिमाइसेस हो या क्लाउड में संग्रहीत होता है, ।
- एन्क्रिप्टेड डेटा के रखरखाव और संचरण के लिए तकनीकी मानकों और संविदात्मक आवश्यकताओं को परिभाषित किया जाना चाहिए।
- क्रिप्टोग्राफिक नियंत्रणों का उपयोग उपकरणों और रखरखाव मीडिया पर संग्रहीत गोपनीय और गुप्त जानकारी की गोपनीयता और अखंडता सुनिश्चित करने के लिए किया जाना चाहिए।
- क्रिप्टोग्राफ़िक नियंत्रणों का उपयोग सभी प्रासंगिक कानूनों और विनियमों के अनुपालन में किया जाना चाहिए।
- जहां भी इलेक्ट्रॉनिक प्रमाणपत्रों का उपयोग किया जाता है, वहां कुंजी निर्माण, वितरण, निरस्तीकरण और रखरखाव के लिए सुरक्षित प्रक्रियाओं को नियोजित किया जाना चाहिए।

- एन्क्रिप्शन तकनीकों का उपयोग करके महत्वपूर्ण सर्वरों या सुरक्षा उपकरणों का प्रबंधन सुरक्षित चैनलों पर किया जाना चाहिए।
- मीडिया के सुरक्षित रखरखाव तक एक्सेस को प्रमाणीकरण (पासवर्ड, बायोमेट्रिक्स, कीपैड) आदि द्वारा नियंत्रित किया जाना चाहिए। संवेदनशील जानकारी वाले प्रिंटआउट सहित संवेदनशील जानकारी के वितरण को न्यूनतम करें।
- पोर्टेबल डिवाइसों में डेटा को एन्क्रिप्ट और पासवर्ड-सुरक्षित करने के लिए रिमूवेबल मीडिया एन्क्रिप्शन सॉफ्टवेयर का उपयोग किया जाना चाहिए।
- सभी नेटवर्कों पर प्रेषित डेटा को सूचना वर्गीकरण के आधार पर अनुमोदित क्रिप्टोग्राफिक एल्गोरिदम का उपयोग करके एन्क्रिप्ट किया जाना चाहिए।
- हडको को संग्रहीत या प्रेषित संवेदनशील या महत्वपूर्ण जानकारी की प्रामाणिकता, अस्वीकृत न होने और अखंडता को सत्यापित करने के लिए इलेक्ट्रॉनिक हस्ताक्षर या संदेश प्रमाणीकरण कोड का उपयोग करना चाहिए।
- एन्क्रिप्शन मानकों और हैशिंग तकनीकों की एक सूची बनाकर अनुमोदित की जानी चाहिए और उसका रखरखाव किया जाना चाहिए।
- सभी पासवर्ड को पासवर्ड फाइलों में गैर-प्रतिवर्ती हैशिंग तकनीकों का उपयोग करके एन्क्रिप्ट किया जाएगा।
- सत्यापन प्रयोजनों के लिए भंडारण में पासवर्ड को सुरक्षित रखने के लिए एक मजबूत क्रिप्टोग्राफिक हैश फ़ंक्शन जो रैंडम साल्ट का उपयोग करता है।
- क्रिप्टोग्राफिक प्रणालियों और परिसंपत्तियों की सुरक्षा के लिए भौतिक और पर्यावरणीय नियंत्रण लागू किए जाने चाहिए।
- मोबाइल उपकरणों के मालिकों को यह सुनिश्चित करना होगा कि निजी तौर पर इस्तेमाल किए जाने वाले मोबाइल उपकरण में कोई आधिकारिक डेटा संग्रहीत न हो। महत्वपूर्ण, संवेदनशील या महत्वपूर्ण व्यावसायिक जानकारी रखने वाले उपकरणों का नियमित बैकअप लिया जाना चाहिए। यह सुनिश्चित किया जाना चाहिए कि मोबाइल उपकरणों का उपयोग करने वाले कर्मचारियों को प्रशिक्षित किया जाए और उन्हें जोखिमों और लागू किए जाने वाले नियंत्रणों के बारे में जागरूक किया जाए।

एन्क्रिप्शन कुंजी प्रबंधन

- एक अनुमोदित कुंजी प्रबंधन प्रक्रिया स्थापित की जाएगी जिसमें कुंजी निर्माण, कुंजी वितरण, कुंजी स्थापना और कुंजी जीवनचक्र प्रबंधन के लिए दिशानिर्देश रेखांकित किए जाएंगे।
- कुंजी प्रबंधन एन्क्रिप्शन और डेटा सुरक्षा का एक महत्वपूर्ण पहलू है, जो एन्क्रिप्शन कुंजियों के सुरक्षित निर्माण, वितरण, भंडारण, रोटेशन और निपटान पर केंद्रित है। एन्क्रिप्शन कुंजियाँ ट्रांजिट डेटा और रेस्ट एन्क्रिप्शन, दोनों के लिए आवश्यक हैं। एन्क्रिप्शन के दौरान प्लेनटेक्स्ट डेटा को सिफरटेक्स्ट में और डिक्रिप्शन के दौरान प्लेनटेक्स्ट डेटा को सिफरटेक्स्ट में बदलने में ये महत्वपूर्ण भूमिका निभाती हैं। एन्क्रिप्टेड डेटा की गोपनीयता, अखंडता और उपलब्धता सुनिश्चित करने और संवेदनशील जानकारी तक अनधिकृत एक्सेस से बचाने के लिए प्रभावी कुंजी प्रबंधन अत्यंत महत्वपूर्ण है।

    a. कुंजी निर्माण: कुंजी निर्माण में यादृच्छिक संख्या जनरेटर या क्रिप्टोग्राफ़िक एल्गोरिदम का उपयोग करके क्रिप्टोग्राफ़िक कुंजियाँ बनाना शामिल है। एन्क्रिप्शन की मज़बूती उत्पन्न कुंजियों की यादृच्छिकता और जटिलता पर निर्भर करती है।
    b. कुंजी वितरण: अधिकृत उपयोगकर्ताओं या प्रणालियों को एन्क्रिप्शन कुंजियों का सुरक्षित वितरण, कुंजी प्रबंधन में एक महत्वपूर्ण कदम है। यह प्रक्रिया सुनिश्चित करती है कि केवल इच्छित प्राप्तकर्ता ही एन्क्रिप्टेड डेटा तक एक्सेस और उसका उपयोग कर सकें।
    c. कुंजी संग्रहण: कुंजियों और परिणामस्वरूप, एन्क्रिप्टेड डेटा तक अनधिकृत एक्सेस को रोकने के लिए एन्क्रिप्शन कुंजियों की सुरक्षा अत्यंत महत्वपूर्ण है। कुंजी संग्रहण में उद्योग की सर्वोत्तम प्रचलन, जैसे हार्डवेयर सुरक्षा मॉड्यूल (HSM) या सुरक्षित कुंजी प्रबंधन प्रणालियों का पालन किया जाना चाहिए।

d. कुंजी रोटेशन: एन्क्रिप्शन कुंजियों को नियमित रूप से बदलने को कुंजी रोटेशन कहा जाता है। यह अभ्यास हमलावरों के लिए चोरी या छेड़छाड़ की गई कुंजियों का फायदा उठाने के अवसर को कम करता है और समग्र डेटा सुरक्षा को बढ़ाता है।
e. कुंजी निरस्तीकरण: संदिग्ध कुंजी समझौता या अनधिकृत एक्सेस के मामलों में, कुंजी निरस्तीकरण प्रशासकों को समझौता की गई कुंजियों को अमान्य करने और बदलने की अनुमति देता है।
f. कुंजी एस्क्रो: कुंजी एस्क्रो में असाधारण स्थितियों में डेटा रिकवरी की सुविधा के लिए विश्वसनीय तृतीय पक्ष के साथ एन्क्रिप्शन कुंजियों को सुरक्षित रूप से संग्रहीत करना शामिल है, जैसे कि जब अधिकृत उपयोगकर्ता अपनी कुंजियों तक एक्सेस खो देते हैं।

स्वीकार्य एन्क्रिप्शन एल्गोरिदम

हडको, प्रयुक्त अनुप्रयोगों के लिए लागू CERT-in/RBI दिशानिर्देशों के अनुसार एन्क्रिप्शन एल्गोरिदम का उपयोग करेगा, उदाहरण के लिए AES (एडवांस एन्क्रिप्शन स्टैंडर्ड), ट्रिपल DES.

शेयरधारकों की भूमिकाएं और जिम्मेदारियां, नीति का प्रवर्तन: - एप्लिकेशन ओनर/सिस्टम इंटीग्रेटर नीति के प्रवर्तन के लिए जिम्मेदार होगा।

डेटा लीक रोकथाम कौशलनीति

हडको के डेटा की लीकेज से सुरक्षा सुनिश्चित करना।

- हडको संवेदनशील (गोपनीय सहित) व्यावसायिक और ग्राहक डेटा/सूचना की सुरक्षा के लिए डेटा हानि/रिसाव रोकथाम कौशलनीति विकसित करेगा।
- डेटा हानि/रिसाव कार्यक्रम में अंतिम पॉइंट डिवाइसों में संसाधित डेटा, ट्रांसमिशन में डेटा, साथ ही सर्वर और अन्य डिजिटल स्टोर में संग्रहीत डेटा, चाहे ऑनलाइन हो या ऑफलाइन, की सुरक्षा शामिल होगी।
- विक्रेता द्वारा प्रबंधित सुविधाओं पर भी डेटा सुरक्षा और संरक्षण सुनिश्चित किया जाना चाहिए।
- आधिकारिक डेटा के अनधिकृत हस्तांतरण से बचने के लिए बाहरी उपकरणों की एक्सेस को प्रतिबंधित करें।

अनधिकृत सॉफ़्टवेयर के निष्पादन को रोकना

हडको में केवल स्वीकृत सॉफ़्टवेयर की स्थापना और उपयोग सुनिश्चित करना और अपनी संचालन प्रणालियों/सूचना प्रसंस्करण सुविधाओं को मेलिशियस सॉफ्टवेर और वायरस के हमलों से बचाने के लिए नियंत्रण स्थापित करेगा ताकि आईटी सेवाएँ निर्बाध रूप से उपलब्ध रहें। सभी एप्लिकेशन/सॉफ़्टवेयर परिनियोजन (हडको परिवेश के भीतर सभी प्रणालियों पर) एक केंद्रीकृत समाधान का उपयोग करके प्रबंधित किए जाएँगे। वित्तीय संस्थान हडको के विक्रेताओं द्वारा जारी नवीनतम सुरक्षा पैच की निगरानी के लिए उपकरण तैनात करेंगे।

सुरक्षित कॉन्फ़िगरेशन

हडको की प्रणालियों को सुरक्षा, विश्वसनीयता और स्थिरता के लिए कॉन्फ़िगर किया जाएगा और ऐसे सभी कॉन्फ़िगरेशन का दस्तावेजीकरण किया जाना चाहिए और कॉन्फ़िगरेशन और समस्या समाधान में कुशल पहचान के लिए प्रणालियों को मानक नामकरण परिपाटी का पालन करना चाहिए।

- हडको को सभी प्रकार के उपकरणों (एंडपॉइंट/वर्कस्टेशन, मोबाइल उपकरण, ऑपरेटिंग सिस्टम, डेटाबेस, एप्लिकेशन, नेटवर्क उपकरण, सुरक्षा उपकरण, सुरक्षा प्रणालियाँ, आदि) पर आधारभूत सुरक्षा आवश्यकताओं/कॉन्फ़िगरेशन को लागू करने के लिए पूरे जीवनचक्र (अवधारणा से लेकर परिनियोजन तक) के दौरान समय-समय पर समीक्षा करते हुए दिशानिर्देश और दस्तावेज़ बनाए रखने चाहिए ।
- बैंक के नेटवर्क में सभी प्रणालियों के लिए सभी महत्वपूर्ण डिवाइस (जैसे फ़ायरवॉल, नेटवर्क स्विच, सुरक्षा उपकरण, आदि) कॉन्फ़िगरेशन और पैच स्तर का समय-समय पर मूल्यांकन किया जाना चाहिए, जिसमें डेटा सेंटर, तृतीय पक्ष द्वारा होस्ट की गई साइटें शामिल हैं।
- सुरक्षित कॉन्फ़िगरेशन दस्तावेज़ों का परीक्षण, परीक्षण वातावरण में किया जाना चाहिए और उत्पादन में जारी करने से पहले अनुमोदित किया जाना चाहिए।
- कम से कम निम्नलिखित के लिए सुरक्षित कॉन्फ़िगरेशन दस्तावेज़ ओईएम और उद्योग पद्दति के आधार पर बनाए जाने चाहिए:
    a. एंडपॉइंट्स
    b. ऑपरेटिंग सिस्टम
    c. वेब सर्वर्स
    d. एप्लीकेशन सर्वर्स
    e. डेटाबेस सर्वर्स
    f. सुरक्षा डिवाइसें
    g. नेटवर्क डिवाइसें
- सुरक्षित कॉन्फ़िगरेशन दस्तावेज़ों की समीक्षा संस्करण में परिवर्तन होने पर, सुरक्षा घटनाओं से प्राप्त सीख के आधार पर या वर्ष में एक बार की जानी चाहिए।

37. डेटा वर्गीकरण

हडको और उसके ग्राहकों दोनों के लिए डेटा संवेदनशीलता के आधार पर ऊपर सूचीबद्ध परिभाषाओं का विस्तृत वर्गीकरण नीचे दिया गया है:

37.1 सार्वजनिक डेटा (हडको और ग्राहक):

परिभाषा: वह डेटा जो सार्वजनिक उपयोग के लिए है और जिसमें संवेदनशील या गोपनीय जानकारी नहीं है।

वर्गीकरण: गैर-संवेदनशील

एक्सेस नियंत्रण: कोई एक्सेस प्रतिबंध नहीं; सार्वजनिक रूप से सुलभ।

उदाहरण (हडको): सार्वजनिक रूप से उपलब्ध विपणन सामग्री, प्रेस विज्ञप्ति, सामान्य वेबसाइट सामग्री।

उदाहरण (ग्राहक): सार्वजनिक रूप से उपलब्ध उत्पाद जानकारी, सामान्य घोषणाएँ।

37.2 आंतरिक डेटा (हडको और ग्राहक):

परिभाषा: वह डेटा जो संगठन के भीतर आंतरिक उपयोग के लिए और इसमें गैर-सार्वजनिक परिचालन जानकारी शामिल हो सकती है।

वर्गीकरण: केवल आंतरिक उपयोग

एक्सेस नियंत्रण: संगठन के भीतर अधिकृत कर्मियों तक सीमित एक्सेस ।
उदाहरण (हडको): आंतरिक संचार, गैर-संवेदनशील आंतरिक रिपोर्ट, परियोजना स्थिति अद्यतन।
उदाहरण (ग्राहक): विशिष्ट विभागों या टीमों के साथ साझा किए गए आंतरिक दस्तावेज़।

37.3 गोपनीय डेटा (हडको और ग्राहक):

परिभाषा: वह डेटा जो संवेदनशील है और जिसे अनधिकृत एक्सेस या प्रकटीकरण से सुरक्षा की आवश्यकता है।
वर्गीकरण: गोपनीय
एक्सेस नियंत्रण: एक्सेस केवल आवश्यकता के आधार पर तथा उचित प्राधिकरण वाले व्यक्तियों तक ही सीमित है।
उदाहरण (हडको): कर्मचारी रिकॉर्ड, वित्तीय डेटा, व्यवसाय योजनाएं, ग्राहक अनुबंध (यदि हडको के साथ साझा किया गया हो)।
उदाहरण (ग्राहक): ग्राहक की व्यक्तिगत जानकारी, वित्तीय रिकॉर्ड, हडको के साथ स्वामित्व संबंधी जानकारी साझा की गई ।

37.4 एग्जीक्यूटिव डेटा (हडको और ग्राहक):

परिभाषा: सबसे संवेदनशील डेटा जिसे इसकी गंभीर प्रकृति के कारण उच्चतम स्तर की सुरक्षा की आवश्यकता होती है।
वर्गीकरण:एग्जीक्यूटिव
एक्सेस नियंत्रण: सख्त प्राधिकरण और अतिरिक्त सुरक्षा उपायों (जैसे, बहु-कारक प्रमाणीकरण) के साथ प्रतिबंधित एक्सेस।
उदाहरण (हडको): बौद्धिक संपदा, व्यापार रहस्य, वित्तीय रिपोर्ट, ग्राहक अनुबंध (यदि हडको के साथ साझा किया गया हो)।
उदाहरण (ग्राहक): स्वामित्व एल्गोरिदम, रणनीतिक योजनाएँ।

38. डार्क वेब मॉनिटरिंग

डार्क वेब मॉनिटरिंग फ्रेमवर्क संवेदनशील संगठनात्मक डेटा और परिसंपत्तियों को संभावित साइबर खतरों से सुरक्षित रखने के लिए महत्वपूर्ण है। डार्क वेब, अवैध गतिविधियों का केंद्र होने के कारण, गोपनीय जानकारी, क्रेडेंशियल्स और अन्य शोषण योग्य डेटा की बिक्री सहित कई जोखिम पैदा करता है।
हडको की डार्क वेब मॉनिटरिंग इस छिपे हुए ऑनलाइन क्षेत्र से उत्पन्न होने वाले खतरों की पहचान, विश्लेषण और शमन के लिए सक्रिय उपायों पर केंद्रित है।
हडको अपने संवेदनशील डेटा, कर्मचारी जानकारी या महत्वपूर्ण व्यावसायिक कार्यों के किसी भी उल्लेख के लिए डार्क वेब फ़ोरम, मार्केटप्लेस और अन्य अवैध प्लेटफ़ॉर्म की निरंतर जाँच के लिए उन्नत उपकरणों और विशिष्ट सेवा प्रदाताओं का उपयोग करेगा। नीति में उल्लंघन किए गए डेटा की पहचान, जोखिमों का आकलन और त्वरित घटना प्रतिक्रिया प्रक्रियाएँ शुरू करने के लिए स्पष्ट प्रोटोकॉल की रूपरेखा दी गई है। डार्क वेब मॉनिटरिंग को आईएस नीति में एकीकृत करके, हडको उभरते साइबर खतरों से आगे रहने और अपने डिजिटल वातावरण की लचीलापन और सुरक्षा सुनिश्चित करने के लिए अपनी प्रतिबद्धता प्रदर्शित करता है।

39. सोशल मीडिया नीति

हडको में सोशल मीडिया गतिविधियों के लिए दिशानिर्देश

परिचय:

ऑनलाइन संचार के आधुनिक युग में, 'सोशल मीडिया' हमारे जीवन का एक अभिन्न अंग बन गया है। यह सूचना, विचार, विश्वास आदि साझा करने का एक आदर्श मंच है। हडको को इस गतिशील संचार माध्यम का उपयोग करने में सक्षम बनाने के लिए, सोशल मीडिया के उपयोग हेतु एक रूपरेखा और दिशानिर्देश तैयार किए गए हैं। ये दिशानिर्देश हडको को सोशल मीडिया के उपयोग हेतु अपनी कौशलनीति बनाने और उसे लागू करने में सक्षम बनाएंगे।

दिशानिर्देश/ढांचे में निम्नलिखित शामिल हैं:

1. उद्देश्य: हडको को सोशल मीडिया का उपयोग क्यों करना चाहिए
2. प्लेटफ़ॉर्म: सोशल मीडिया के अंतर्गत उपलब्ध उपकरण
3. शासन: सहभागिता के नियम क्या हैं?
4. संचार कौशलनीति: सभी हितधारकों के साथ कैसे बातचीत करें
5. सहभागिता: एक समुदाय को कैसे बनाएं रखें
6. संस्थागतकरण: संगठन संरचना में सोशल मीडिया को कैसे शामिल किया जाए

1. उद्देश्य:

हडको के सोशल मीडिया प्लेटफॉर्म/हैंडल्स का मुख्य उद्देश्य होगा:

- ऑनलाइन सोशल साइट्स/चैनलों के माध्यम से कंपनी के बारे में जागरूकता बढ़ाएं और इस क्षेत्र में आगे के विकल्पों का भी पता लगाएं।
- अधिक सदस्यों को जोड़कर, 'लाइक' उत्पन्न करके, हडको के आधिकारिक हैंडल (मंत्रालय से प्राप्त दिशानिर्देशों के अनुसार) या सदस्यों द्वारा महत्वपूर्ण ट्वीट्स / फेसबुक शेयर को रीट्वीट करके व्यापक दर्शक आधार बनाएं।
- वीडियो/फोटोग्राफ/एवी आदि के रूप में नवीनतम जानकारी प्रदर्शित करें।
- आवश्यकता पड़ने पर और उपयुक्त समझे जाने पर विभिन्न शेयरधारकों और सामान्य जनता को बधाई/राय/प्रतिक्रिया आदि व्यक्त करने के लिए प्रबंधन को संदेश भेजने के लिए मंच प्रदान करना।

2. प्लेटफ़ॉर्म:

हडको द्वारा वर्तमान में निम्नलिखित सोशल मीडिया प्लेटफॉर्म का उपयोग किया जा रहा है:

नाम	प्रकार	टिप्पणी
फेसबुक	सोशल नेटवर्किंग वेबसाइट	आधिकारिक अकाउंट **https://www.facebook.com/HUDCO**
X.com (पूर्व में ट्विटर)	ऑनलाइन समाचार और सामाजिक नेटवर्किंग सेवा जहां उपयोगकर्ता संदेश पोस्ट करते हैं और उनसे बातचीत करते हैं, जिन्हें "ट्वीट" के रूप में जाना जाता है।	आधिकारिक अकाउंट **https://twitter.com/hudcolimited**
यूट्यूब	यूट्यूब एक वीडियो शेयरिंग वेबसाइट है जो ऑनलाइन वीडियो देखना आसान बनाती है। इस पर वीडियो बनाकर अपलोड किए जा सकते हैं और दूसरों के साथ शेयर किए जा सकते हैं।	आधिकारिक अकाउंट **https://www.youtube.com/hudcoltd**
लिंक्डइन	लिंक्डइन एक व्यवसाय और रोजगार-केंद्रित सोशल मीडिया प्लेटफॉर्म है जो वेबसाइटों और मोबाइल ऐप के माध्यम से काम करता है। इस प्लेटफ़ॉर्म का उपयोग मुख्य रूप से प्रोफेशनल नेटवर्किंग और करियर विकास के लिए किया जाता है, जो नौकरी चाहने वालों को अपना बायोडाटा पोस्ट करने और नियोक्ताओं को नौकरियाँ पोस्ट करने की अनुमति देता है।	आधिकारिक अकाउंट **https://www.linkedin.com/company/hudco- limited**
इंस्टाग्राम	इंस्टाग्राम एक मोबाइल, डेस्कटॉप और इंटरनेट आधारित फोटो शेयरिंग एप्लीकेशन और सेवा है जो उपयोगकर्ताओं को पूर्व-अनुमोदित अनुयायियों के साथ सार्वजनिक या निजी रूप से तस्वीरें और वीडियो साझा करने की अनुमति देता है।	आधिकारिक अकाउंट बनाया जा सकता है

3. नियंत्रण:

3.1 संसाधन नियंत्रण:

मीडिया में तेजी से हो रहे विकास के साथ तालमेल बनाए रखने और सहभागिता का प्रबंधन करने के लिए आउटसोर्स संसाधनों सहित एक समर्पित सोशल मीडिया टीम का गठन किया जा सकता है।

a) भूमिकाएं और जिम्मेदारियां:

i) आधिकारिक सोशल मीडिया हैंडल केवल पीआर यूनिट द्वारा बनाए और बनाए रखे जाएंगे।
ii) पीआर इकाई सभी सामग्री को संकलित, संपादित और प्रारूप तैयार करेगा।
iii) पीआर यूनिट द्वारा सोशल मीडिया साइटों पर अपलोडिंग / प्रतिक्रिया / निगरानी।
iv) प्रत्येक ऑनलाइन सोशल मीडिया प्लेटफॉर्म पर हडको का एक आधिकारिक अकाउंट होगा, जिसका प्रबंधन पीआर यूनिट द्वारा केंद्रीय रूप से किया जाएगा।

v) कर्मचारियों को सभी आधिकारिक सोशल मीडिया हैंडल से जुड़ने के लिए प्रोत्साहित किया जाएगा और एक्सेस बढ़ाने के लिए पोस्ट और जानकारी को शेयर / रीट्वीट / लाइक करने के लिए भी याद दिलाया जाएगा।

vi) कर्मचारियों को ऑनलाइन मीडिया के उपयोग/ऑनलाइन व्यवहार के संबंध में संलग्न अनुलग्नक-I में दिए गए दिशानिर्देशों का पालन करना होगा। आवश्यकतानुसार दिशानिर्देशों में संशोधन किया जाएगा।

b) जवाबदेही:

सोशल मीडिया का उपयोग करने वाले नागरिकों के साथ संपर्क के लिए नामित अधिकारियों को आरटीआई अधिनियम और आईटी संशोधन अधिनियम, 2008 के अनुरूप प्रावधानों के अंतर्गत कवर किया जाएगा।

3.2 अकाउंट नियंत्रण:

i) **अकाउंट बनाना :** एक सोशल मीडिया अकाउंट किसी संगठन की ऑनलाइन पहचान स्थापित करता है। जहाँ तक संभव हो, इंटरनेट पर खोज को आसान बनाने के लिए विभिन्न सोशल नेटवर्किंग खातों के लिए एक ही नाम अपनाया जा सकता है। खाता नाम 15 अक्षरों से ज़्यादा नहीं होना चाहिए (जैसे, ट्विटर)।

ii) **लॉगिन और पासवर्ड:** प्रत्येक नए अकाउंट के लिए एक यूआरएल, उपयोगकर्ता नाम और/या ईमेल पता और पासवर्ड की आवश्यकता होती है। लॉगिन आईडी और पासवर्ड का उचित रिकॉर्ड रखना आवश्यक है। यह महत्वपूर्ण है क्योंकि विभाग की ओर से पोस्ट करने के लिए कई लोगों को अधिकृत किया जा सकता है।

iii) **अकाउंट की स्थिति:** यह परिभाषित करना महत्वपूर्ण है कि क्या यह कार्य केवल आधिकारिक अकाउंट के माध्यम से किया जा सकता है या अधिकारियों को आधिकारिक प्रतिक्रियाएँ पोस्ट करने के लिए व्यक्तिगत अकाउंट का उपयोग करने की भी अनुमति दी जा सकती है। यह निर्धारित करता है कि हडको की ओर से कौन क्या कहता है और उसे किस रूप में प्रकाशित किया जाता है और यह भी बताता है कि प्रकाशित जानकारी के प्रत्येक भाग को प्रकाशन स्थल पर कैसे प्रस्तुत किया जाता है। सबसे महत्वपूर्ण पहलू यह है कि प्रतिक्रियाएँ आधिकारिक या व्यक्तिगत क्षमता में हैं।

3.3 प्रतिक्रिया नियंत्रण:

सोशल मीडिया का मुख्य आकर्षण प्रतिक्रिया और फीडबैक की सहजता और तत्कालता है । साइट पर आने वाले लोग पूर्व-निर्धारित समय सीमा के भीतर किसी प्रकार की प्रतिक्रिया की अपेक्षा करते हैं।

i) सभी उत्तर संक्षिप्त एवं सारगर्भित होने चाहिए।

ii) सोशल मीडिया प्लेटफॉर्म के माध्यम से उपयोगकर्ताओं के लिए सटीक, पूर्ण, विनम्र और त्वरित फीडबैक प्रणाली।

iii) ककार्मिकों को व्यक्तिगत क्षमता में जवाब देना से मना किया गया है।

iv) हडको से संबंधित वार्तालापों पर नज़र रखने के लिए उचित ट्रैकिंग प्रणाली का उपयोग करके निगरानी की जाएगी।

v) स्पैम, विज्ञापनों और अनुचित सामग्री से बचने के लिए साइटों का संचालन करना। प्रासंगिक और संबंधित कीवर्ड के लिए सोशल मीडिया नेटवर्क पर नज़र रखना और सोशल मीडिया साइटों पर सकारात्मक बातचीत शुरू करने के लिए उन पर प्रतिक्रिया देना।

3.4 सामग्री नियंत्रण:

i) **सामग्री तैयार करना:** दर्शकों की रुचि के लिए कहानियाँ/फोटो तैयार करना। साइट के लिए सामग्री संक्षिप्त और विशिष्ट होनी चाहिए जिस पर इसे प्रकाशित किया जा रहा है।

ii) **सुगम्यता:** व्यापक भागीदारी के लिए, सामग्री की उपलब्धता भारतीय भाषाओं में होनी चाहिए और इसे केवल पाठ तक सीमित नहीं रखा जाना चाहिए। सामग्री में वेबसाइट के लिए भारत सरकार के दिशानिर्देशों का पालन होना चाहिए और भारतीय भाषाओं में सुगम्यता के साथ-साथ दिव्यांगजनों के लिए सामग्री की सुगम्यता से संबंधित चुनौतियों का पर्याप्त रूप से समाधान किया जाना चाहिए।

iii) **मॉडरेशन:** मॉडरेशन में कॉपीराइट, जोड़ने और हटाने के अधिकार आदि से संबंधित मामले शामिल होने चाहिए।

iv) **अभिलेख प्रबंधन:** जब कोई भी जानकारी ऑनलाइन साझा की जाती है या कोई मार्गदर्शन दिया जाता है, तो यह सुनिश्चित करना आवश्यक है कि सभी प्रासंगिक डिजिटल अभिलेख एकत्र किए जाएँ, उनका पता लगाया जाए और अभिलेखों का उचित प्रबंधन किया जाए। यह महत्वपूर्ण है कि डिजिटल अभिलेख रखने के नियम पहले ही बता दिए जाएँ ताकि ऐतिहासिक डेटा चाहने वालों को विधिक और सीमाओं की जानकारी हो। चूँकि अधिकांश सोशल मीडिया प्लेटफ़ॉर्म भारत के बाहर स्थित हैं और भारतीय विधिक द्वारा शासित या भारतीय नियमों द्वारा प्रबंधित और नियंत्रित नहीं हैं, इसलिए सूचना सुरक्षा और संग्रहण पर ध्यान देने की आवश्यकता है। यदि आवश्यक हो, तो हडको (आंतरिक रूप से/बाहरी सोशल मीडिया सेवा प्रदाता के माध्यम से) निम्नलिखित के लिए शिकायत और प्रतिक्रिया प्रणाली हेतु सेवा स्तर समझौते तैयार कर सकता है:

- सामग्री संग्रहण
- सामग्री तक साझा एक्सेस
- अभिलेखीय प्रणाली

v) **डेटा एवं सूचना सुरक्षा नियंत्रण:**

हडको द्वारा सोशल मीडिया के माध्यम से नागरिकों के साथ किए जाने वाले संचार में भी उसी डेटा प्रतिधारण नीति का पालन किया जाना चाहिए जो अन्य इलेक्ट्रॉनिक और गैर-इलेक्ट्रॉनिक माध्यमों से किए जाने वाले संचार में अपनाई जाती है। डेटा पोर्टेबिलिटी अनुपालन एक सोशल मीडिया प्लेटफ़ॉर्म से दूसरे में भिन्न होता है।

व्यक्तिगत सूचना एवं सुरक्षा से संबंधित प्रावधान: सूचना प्रौद्योगिकी अधिनियम 2000 के अंतर्गत, केंद्र सरकार ने सोशल मीडिया को प्रभावित करने वाले विभिन्न नियम और विनियम बनाए हैं। इस संबंध में कुछ सबसे महत्वपूर्ण प्रावधान इस प्रकार हैं:

a) सूचना प्रौद्योगिकी (उचित सुरक्षा पद्धतियाँ एवं प्रक्रियाएँ तथा संवेदनशील व्यक्तिगत डेटा या सूचना) नियम 2011 व्यक्तिगत सूचना एवं सुरक्षा के प्रावधानों और संवेदनशील व्यक्तिगत डेटा की परिभाषा देते हैं। किसी व्यक्ति के संवेदनशील व्यक्तिगत डेटा या सूचना से तात्पर्य ऐसी व्यक्तिगत सूचना से है जिसमें निम्नलिखित से संबंधित जानकारी शामिल हो:

पासवर्ड; वित्तीय जानकारी जैसे बैंक खाता या क्रेडिट कार्ड या डेबिट कार्ड या अन्य भुगतान साधन विवरण; शारीरिक, दैहिक और मानसिक स्वास्थ्य स्थिति; यौन अभिविन्यास; चिकित्सा रिकॉर्ड और इतिहास; बायोमेट्रिक जानकारी।

बशर्ते कि, कोई भी सूचना जो सार्वजनिक डोमेन में स्वतंत्र रूप से उपलब्ध या सुलभ है या सूचना का अधिकार अधिनियम, 2005 या उस समय लागू किसी अन्य कानून के तहत प्रस्तुत की गई है, उसे इन नियमों के प्रयोजनों के लिए संवेदनशील व्यक्तिगत डेटा या सूचना नहीं माना जाएगा।

b) ऐसे संवेदनशील व्यक्तिगत डेटा की सुरक्षा के प्रयोजनों के लिए, सरकार ने यह अनिवार्य किया है कि कोई भी कानूनी इकाई जो संवेदनशील व्यक्तिगत डेटा का प्रसंस्करण, व्यवहार या प्रबंधन कर रही है, उसे उचित सुरक्षा और प्रक्रियाओं को लागू करना होगा।

c) इसके अलावा, सूचना प्रौद्योगिकी (मध्यस्थ दिशानिर्देश) नियम 2011 के तहत, चूंकि उक्त सरकारी विभाग जो सोशल मीडिया सुविधाएं प्रदान कर रहा है, एक मध्यस्थ है, इसलिए उसे सूचना प्रौद्योगिकी (मध्यस्थ दिशानिर्देश) नियम 2011 का अनुपालन करना होगा। उक्त नियमों के नियम 3(4) के तहत, सरकारी विभाग प्रभावित व्यक्ति से लिखित शिकायत प्राप्त होने पर छत्तीस घंटे के भीतर कार्रवाई करेगा और जहां लागू हो, ऐसी जानकारी के उपयोगकर्ता या मालिक के साथ मिलकर ऐसी जानकारी को निष्क्रिय करने के लिए काम करेगा जो उप-नियम (2) का उल्लंघन करती है।

d) इसके अतिरिक्त, सरकारी विभाग ऐसी सूचना और संबंधित अभिलेखों को जांच के प्रयोजनार्थ कम से कम नब्बे दिनों तक सुरक्षित रखेगा।

vi) गोपनीयता और डेटा संग्रहण के नियम:

लोगों को अनुचित या आपत्तिजनक सामग्री के संपर्क से बचाना सुनिश्चित करना महत्वपूर्ण है।

a) चूंकि सोशल नेटवर्क पर प्रोफाइल अक्सर व्यक्तियों से जुड़ी होती हैं, न कि संगठनों से, इसलिए संगठन की साइट/पेज के लिए एक अलग कार्य प्रोफाइल बनाई जा सकती है, जिसे फिर एक सामान्य ईमेल पते से जोड़ा जा सकता है, जो टीम में किसी के लिए भी सुलभ हो, जिससे वे व्यक्तिगत गोपनीयता से समझौता किए बिना सोशल नेटवर्क का प्रबंधन कर सकें।

b) यह महत्वपूर्ण है कि संगठन की सोशल मीडिया नीति डेटा सुरक्षा और गोपनीयता से संबंधित मौजूदा विधिक के अनुरूप हो। हडको के प्रत्येक विभाग को नागरिकों की गोपनीयता की सुरक्षा के लिए अतिरिक्त सुरक्षा उपाय करने के साथ-साथ पारदर्शिता के उच्चतम स्तर को बनाए रखने की भी की सिफ़ारिश की जा सकती है।

4. संचार कौशलनीति:

i. सोशल मीडिया का उपयोग केवल हडको द्वारा मौजूदा जानकारी को संप्रेषित करने और जनता तक आधिकारिक नीति/सूचना का प्रचार करने के लिए किया जा सकता है।

ii. सोशल मीडिया हैंडल को सूचनाप्रद/रोचक बनाया जाएगा, जिसमें नियमित समाचार/घटना अपडेट के अलावा और भी कहानियां शामिल होंगी।

5. सहभागिता विश्लेषण:

i. सोशल मीडिया उपस्थिति की नियमित निगरानी और मूल्यांकन करें।

ii. सकारात्मक, तटस्थ या नकारात्मक भावनाओं के लिए बातचीत, लिंक और ब्लॉग पर नज़र रखें। यदि नकारात्मक भावनाएँ पाई जाती हैं, तो उन्हें दूर करने के लिए एक योजना तैयार करें।

iii. संबंधित से सूचना एकत्रित करने के बाद प्रश्नों का उत्तर देना।

6. सोशल मीडिया को संस्थागत बनाएं:

i. नियम स्थापित किए जा सकते हैं कि सभी नीतिगत घोषणाएं पारंपरिक तरीके से एक साथ सोशल मीडिया पर भी की जाएंगी।

ii. सभी महत्वपूर्ण अवसरों पर, जहां तक संभव हो, दस्तावेजों को सोशल मीडिया का उपयोग करके प्रसारित किया जा सकता है।

iii. वेबसाइट से सभी अपडेट को अधिमानतः सोशल मीडिया साइटों पर अपडेट किया जाना चाहिए।

7. निष्कर्ष:

हडको को अपने विभिन्न शेयरधारकों के साथ अधिक सार्थक रूप से जुड़ने के लिए सोशल मीडिया प्लेटफार्मों का उपयोग करने में सहायता करने के उद्देश्य से तैयार किए गए हैं।

हडको के कार्मिकों के लिए मानक दिशानिर्देश

1) कार्मिकों को यह ध्यान रखना चाहिए कि फेसबुक/ट्विटर/इंस्टाग्राम जैसे सोशल मीडिया प्लेटफॉर्म सामान्य जनता के लिए स्वतंत्र रूप से उपलब्ध और आसानी से सुलभ हैं। इसलिए कार्मिकों को ज़िम्मेदारी से काम करना और ऐसी कोई भी जानकारी पोस्ट/प्रकाशित/टिप्पणी/रिलीज़ नहीं करनी चाहिए जो हडको की समग्र छवि के लिए गोपनीय/संवेदनशील/हानिकारक हो।

2) कार्मिकों को ऐसी सामग्री पोस्ट करते समय अपने सर्वोत्तम विवेक का प्रयोग करना चाहिए जो न तो अनुचित हो और न ही हडको के लिए हानिकारक हो।

3) अनुचित सोशल मीडिया व्यवहार के उदाहरणों में ऐसी टिप्पणियां पोस्ट करना शामिल है जो नकारात्मक, अपमानजनक, मालिकाना, उत्पीड़नकारी और अपमानजनक हों या जो शत्रुतापूर्ण कार्य वातावरण बना सकती हों।

4) सोशल मीडिया नेटवर्क, ब्लॉग और अन्य प्रकार की ऑनलाइन सामग्री कभी-कभी प्रेस और मीडिया का ध्यान आकर्षित या विधिक प्रश्न उत्पन्न करती है। कार्मिकों को इन प्रश्नों को अधिकृत प्रवक्ताओं को भेजना चाहिए।
5) यदि कार्मिकों को सोशल मीडिया का उपयोग करते समय ऐसी स्थिति/बातचीत का सामना करना पड़ता है, जो शत्रुतापूर्ण होने का खतरा पैदा करती है, तो कार्मिकों को विनम्र तरीके से बातचीत से अलग हो जाना चाहिए।
6) वर्तमान या पूर्व कार्मिकों को, सदस्यों, विक्रेताओं या आपूर्तिकर्ताओं की ईमेज का संदर्भ देने या पोस्ट करने से पहले उचित अनुमति लेनी चाहिए। इसके अतिरिक्त, कार्मिकों को किसी तृतीय पक्ष के कॉपीराइट, कॉपीराइट सामग्री, ट्रेडमार्क, सेवा चिह्न या अन्य बौद्धिक संपदा का उपयोग करने से पहले उचित अनुमति लेनी चाहिए।
7) कार्मिकों को यह ध्यान रखना चाहिए कि फेसबुक/ट्विटर/इंस्टाग्राम जैसे सोशल मीडिया प्लेटफॉर्म सामान्य जनता के लिए स्वतंत्र रूप से उपलब्ध और आसानी से सुलभ हैं। इसलिए कार्मिकों को ज़िम्मेदारी से काम करना चाहिए और ऐसी कोई भी जानकारी पोस्ट/प्रकाशित/टिप्पणी/रिलीज़ नहीं करनी चाहिए जो हडको की समग्र छवि के लिए गोपनीय/संवेदनशील/हानिकारक हो।
8) कार्मिकों को ऐसी सामग्री पोस्ट करते समय अपने सर्वोत्तम विवेक का प्रयोग करना चाहिए जो न तो अनुचित हो और न ही हडको के लिए हानिकारक हो।
9) सोशल मीडिया व्यवहार के उदाहरणों में ऐसी अनुचित टिप्पणियां पोस्ट करना शामिल है जो नकारात्मक, अपमानजनक, मालिकाना, उत्पीड़नकारी और अपमानजनक हों या जो शत्रुतापूर्ण वातावरण बना सकती हों।
10) सोशल मीडिया नेटवर्क, ब्लॉग और अन्य प्रकार की ऑनलाइन सामग्री कभी-कभी प्रेस और मीडिया का ध्यान आकर्षित करती है या विधिक प्रश्न उत्पन्न करती है। कार्मिकों इन प्रश्नों को अधिकृत प्रवक्ताओं को भेजना चाहिए।
11) यदि सोशल मीडिया का उपयोग करते समय कर्मचारियों को ऐसी स्थिति/बातचीत का सामना करना पड़ता है, जो शत्रुतापूर्ण होने का खतरा पैदा करती है, तो कर्मचारियों को विनम्र तरीके से बातचीत से अलग हो जाना चाहिए।
12) वर्तमान या पूर्व कार्मिकों, सदस्यों, विक्रेताओं या आपूर्तिकर्ताओं की तस्वीरों का संदर्भ देने या पोस्ट करने से पहले उचित अनुमति लेनी चाहिए। इसके अतिरिक्त, कार्मिकों को किसी तृतीय पक्ष के कॉपीराइट, कॉपीराइट सामग्री, ट्रेडमार्क, सेवा चिह्न या अन्य बौद्धिक संपदा का उपयोग करने से पहले उचित अनुमति लेनी चाहिए। सोशल मीडिया का उपयोग हडको में कार्मिकों की ज़िम्मेदारियों में हस्तक्षेप नहीं करना चाहिए।

40. पूर्वनियोजित आंतरिक हमलों से बचाव

स्टाफ का कोई सदस्य गोपनीय जानकारी को निशाना बना सकता है या संगठन की वेबसाइट को खराब कर सकता है, जिसके परिणामस्वरूप वित्तीय नुकसान और शर्मिंदगी दोनों हो सकती है, इसलिए ऐसी गतिविधि को नियंत्रित करने की नीति में निम्नलिखित उपाय शामिल होने चाहिए।

- भूमिकाओं और आवश्यकताओं के अनुसार सूचना तक एक्सेस होना चाहिए।
- हडको की भर्ती और नियुक्ति प्रक्रियाओं में निम्नलिखित शामिल होने चाहिए:

  पृष्ठभूमि जाँच

  गोपनीयता/गैर-प्रकटीकरण समझौता

  चोरी आदि के कारण होने वाली हानि से सुरक्षा के लिए कार्मिकों की बाध्यता।

41. अनुपालन

यह आवश्यक है कि हडको सभी प्रासंगिक वैधानिक, विनियामक और संविदात्मक आवश्यकताओं को परिभाषित, दस्तावेजित और अनुरक्षित करे तथा प्रत्येक सूचना प्रणाली के लिए इन आवश्यकताओं को पूरा करने हेतु संगठन का दृष्टिकोण अपनाए।

41.1 विधिक और संविदात्मक आवश्यकता का अनुपालन

आवश्यक है कि विधिक और अनुपालन व्यवसाय संचालन के लिए प्रासंगिक विधिक, विनियमन और अनुपालन आवश्यकताओं की पहचान करें।

कार्यात्मक प्रमुखों को यह सुनिश्चित करना आवश्यक है कि उनका कार्य सूचना और साइबर सुरक्षा नीति और प्रासंगिक नियंत्रणों की आवश्यकताओं को पूरा करता है।

41.2 लागू विधिक और संविदात्मक आवश्यकताओं की पहचान

- सभी प्रासंगिक वैधानिक, विनियामक और संविदात्मक आवश्यकताओं की सूची के साथ-साथ व्यक्तिगत जिम्मेदारियों को भी परिभाषित किया जाना चाहिए।
- यह सुनिश्चित करने के लिए समय-समय पर समीक्षा की जानी चाहिए कि पहचान की गई वैधानिक, विनियामक और संविदात्मक आवश्यकताओं की सूची, व्यक्तिगत जिम्मेदारियों के साथ, अद्यतन रहे।

41.3 बौद्धिक संपदा अधिकार

- सॉफ्टवेयर अधिग्रहण ज्ञात और प्रतिष्ठित स्रोतों के माध्यम से किया जाना चाहिए ताकि यह सुनिश्चित किया जा सके कि कॉपीराइट का उल्लंघन न हो।
- हडको प्रबंधन को बौद्धिक संपदा के रूप में पहचानी गई जानकारी पर अपना समर्थन प्रदान करना आवश्यक है। बौद्धिक संपदा अधिकार (आईपीआर) को सभी अनुबंधों में शामिल किया जाना है, और इसे निम्नलिखित सुनिश्चित करने के लिए लागू किया जाता है, लेकिन इन्हीं तक सीमित नहीं:
- ऐसी सामग्री के उपयोग पर विधायी, विनियामक और संविदात्मक आवश्यकताओं का अनुपालन जिसके संबंध में आईपीआर हो सकता है।
- सॉफ्टवेयर या दस्तावेज़ कॉपीराइट, डिज़ाइन अधिकार, ट्रेडमार्क, पेटेंट और स्रोत कोड लाइसेंस सहित आईपीआर का उल्लंघन नहीं किया जाता है।
- हडको के नेटवर्क परिवेश में केवल लाइसेंस प्राप्त सॉफ़्टवेयर ही स्थापित किए जाने हैं।
  सभी सॉफ़्टवेयर लाइसेंसों का रिकॉर्ड और नियमित रूप से अद्यतन किया जाना चाहिए।
- सर्वोत्तम प्रयास के आधार पर, यह सुनिश्चित किया जाएगा कि तृतीय पक्ष सेवा प्रदाता द्वारा प्रदान किए गए सभी अनुप्रयोगों या अनुप्रयोगों में परिवर्तनों के लिए बौद्धिक संपदा अधिकार हडको के पास ही रहें।

41.4 अभिलेखों का सुरक्षा

किसी संगठन के महत्वपूर्ण अभिलेखों को हानि, विनाश, अनधिकृत एक्सेस, गैरकानूनी और अनधिकृत प्रतिलिपिकरण, छेड़छाड़ और जालसाजी से सुरक्षित रखा जाना चाहिए, और कुछ मामलों में कुछ अभिलेखों को निश्चित अवधि के लिए रखना कानूनन आवश्यक है। हालाँकि, सभी अभिलेखों को हमेशा के लिए सुरक्षित रखना संभव या वांछनीय नहीं है।

- यह आवश्यक है कि प्रासंगिक विधिक, विनियमों और, यदि लागू हो, तो संविदात्मक धाराओं के अनुसार डेटा संरक्षण और गोपनीयता सुनिश्चित की जाए।
- किसी दस्तावेज़ या मेल में उल्लिखित व्यक्तिगत पहचान पत्र या सूचना, जिसका उपयोग अकेले या अन्य सूचना के साथ किसी व्यक्ति की पहचान करने, उससे संपर्क करने या उसका पता लगाने के लिए किया जा सकता है, को गोपनीय माना जाएगा।
- जहाँ भी संभव हो, जानकारी को संगठन की सीमाओं से बाहर जाने से बचाने के लिए डेटा हानि निवारण समाधान लागू किया जाएगा।
- पीआईआई को एकत्रित करने, उपयोग करने और संग्रह के लिए प्रासंगिक विधिक, विनियमन और संविदात्मक खंडों की पहचान की जानी है।
- यह आवश्यक है कि जिस उद्देश्य के लिए व्यक्तिगत पहचान पत्र (पीआईआई) एकत्र किया गया था, उसे ऑनर द्वारा पहचाना जाए। ऑनर को उद्देश्य के अनुसार स्वयं समीक्षा और किसी भी विचलन की रिपोर्ट करनी होगी, जिसके लिए मूल कारण विश्लेषण (आरसीए) के आधार पर उचित कार्रवाई की जानी है।
- यह आवश्यक है कि व्यक्तिगत पहचान संबंधी प्रासंगिक जानकारी (पीईआई) तक केवल आधिकारिक मान्यता ही उपलब्ध हो। यह सुनिश्चित किया जाना चाहिए कि यह प्राधिकरण व्यावसायिक कार्य द्वारा प्रदान किया गया हो।
- पीआईआई को नेटवर्क ड्राइव और/या एप्लिकेशन डेटाबेस में सुदृढ़ एक्सेस नियंत्रण उपायों (उदाहरण के लिए उपयोगकर्ता आईडी/पासवर्ड) के साथ संग्रहीत किया जाएगा और केवल उन व्यक्तियों को उपलब्ध कराया जाएगा जिनकी वैध और अनुमोदित व्यावसायिक आवश्यकता है।
- डेटा उल्लंघन से संबंधित सभी घटनाएं, जिनके परिणामस्वरूप पहचान की चोरी हो सकती है, की जांच और समापन के लिए सूचना सुरक्षा समिति द्वारा समन्वय किया जाएगा।
- यदि पीआईआई को इंटरनेट पर प्रेषित करने की आवश्यकता है, तो यह सुनिश्चित किया जाएगा कि इसे एन्क्रिप्शन विधियों का उपयोग करके भेजा जाए।

41.5 गोपनीयता और व्यक्तिगत रूप से पहचान योग्य जानकारी की सुरक्षा

अनधिकृत एक्सेस, संचरण, प्रकाशन, क्षति, उपयोग, संशोधन, प्रकटीकरण और हानि के विरुद्ध डेटा संरक्षण और गोपनीयता (जैसे ग्राहक विवरण, प्रतिबंधित डेटा आदि) को हडको में पर्याप्त तकनीकी और प्रशासनिक नियंत्रण लागू करके सुनिश्चित किया जाना है।

41.6 क्रिप्टोग्राफ़िक नियंत्रणों का विनियमन

- यह आवश्यक है कि क्रिप्टोग्राफ़िक नियंत्रणों का उपयोग सभी प्रासंगिक समझौतों, विधिक और विनियमों के अनुपालन में किया जाए।
- एन्क्रिप्शन कुंजी डेटा तक एक्सेस केवल अधिकृत प्रशासकों तक ही सीमित रहेगी। यह सुनिश्चित किया जाएगा कि ऐसे संवेदनशील डेटा तक पहुँच रखने वाले प्रशासकों की गतिविधियों को उचित रूप से लॉग किया जाए और समय-समय पर उनकी निगरानी की जाए।

अनुलग्नक I – शब्दावली

टर्म	विवरण
एएमसी	वार्षिक रखरखाव अनुबंध
बीसीएम	व्यवसाय निरंतरता प्रबंधन
बीसीपी	व्यवसाय निरंतरता योजना
सीसीटीवी	क्लोज्ड सर्किट टेलीविजन
सीडी	कॉम्पेक्ट डिस्क
सीआईएसओ	मुख्य सूचना सुरक्षा अधिकारी
सीओटीएस	शेल्फ के वाणिज्यिक
सीटीओ	मुख्य प्रौद्योगिकी अधिकारी
डीसी	डेटा सेंटर
डीएमजेड	विसैन्यीकृत क्षेत्र
डीआरपी	आपदा पुनर्प्राप्ति योजना
डीवीडी	डिजिटल वीडियो डिस्क
ईआरटी	इमरजेंसी रिस्पांस टीम
एचआर	मानव संसाधन
आईडी	पहचानकर्ता
आईपी	इंटरनेट प्रोटोकॉल
आईपीआर	बौद्धिक संपदा अधिकार
आईएस	सूचना सुरक्षा
आईइसएम	सूचना सुरक्षा प्रबंधक
आईइसपी	सूचना और साइबर सुरक्षा नीति
आईटी	सूचना प्रौद्योगिकी
एलएएन	लोकल एरिया नेटवर्क
पीआईआई	व्यक्तिगत रूप से पहचान योग्य जानकारी का अर्थ है किसी व्यक्ति से संबंधित कोई भी जानकारी, जो प्रत्यक्ष या अप्रत्यक्ष रूप से, किसी निगमित निकाय के पास उपलब्ध या संभावित अन्य जानकारी के साथ मिलकर, उस व्यक्ति की पहचान जैसे: नाम, पता, फ़ोन नंबर आदि करने में सक्षम हो।
हडको	हाउसिंग एंड अर्बनडेवलपमेंट कॉर्पोरेशन

टर्म	विवरण
आरपीओ	पुनर्प्राप्ति बिंदु उद्देश्य
आरसीए	मूल कारण विश्लेषण
आरटीओ	पुनर्प्राप्ति समय उद्देश्य
एसएफटीपी	सुरक्षित फ़ाइल स्थानांतरण प्रोटोकॉल
एसपीआई	संवेदनशील व्यक्तिगत सूचना से तात्पर्य ऐसी व्यक्तिगत सूचना से है जिसमें निम्नलिखित से संबंधित सूचना शामिल है; (i) पासवर्ड; (ii) वित्तीय सूचना जैसे बैंक खाता या क्रेडिट कार्ड या डेबिट कार्ड या अन्य भुगतान साधन विवरण; (iii) शारीरिक, दैहिक और मानसिक स्वास्थ्य स्थिति; (iv) यौन अभिविन्यास; (v) चिकित्सा रिकॉर्ड और इतिहास; (vi) बायोमेट्रिक सूचना; (vii) सेवा प्रदान करने के लिए निगमित निकाय को प्रदान किए गए उपरोक्त खंडों से संबंधित कोई विवरण; और (viii) वैध अनुबंध के तहत या अन्यथा प्रसंस्करण, संग्रहीत या संसाधित करने के लिए निगमित निकाय द्वारा उपरोक्त खंडों के तहत प्राप्त कोई भी सूचना।
एसएलए	सेवा स्तर समझौता
एसओपी	मानक संचालन प्रक्रिया
एसओपीसी	संपर्क का एकल बिंदु
एसएसएल	सिक्योर सॉकेट परत
टीपीए	तृतीय पक्ष मूल्यांकन
यूपीएस	निर्बाध विद्युत आपूर्ति
वीएलएएन	वर्चुअल लोकल एरिया नेटवर्क
वीपीएन	वर्चुअल प्राइवेट नेटवर्क
डब्ल्यूएएन	वाइड एरिया नेटवर्क

अनुलग्नक II - संदर्भ

क्रम सं.	परिपत्र संदर्भ संख्या	विवरण
1.	आईएसओ 27001:2013 ढांचा	यह सूचना सुरक्षा प्रबंधन प्रणाली की स्थापना, कार्यान्वयन, रखरखाव और निरंतर सुधार के लिए आवश्यक है।
2.	आईटी अधिनियम 2000	इलेक्ट्रॉनिक डेटा इंटरचेंज और इलेक्ट्रॉनिक संचार के अन्य साधनों द्वारा किए गए लेनदेन को कानूनी मान्यता प्रदान करने के लिए एक अधिनियम।
3.	आईटी संशोधन अधिनियम 2008	यह आईटी अधिनियम 2000 में महत्वपूर्ण संशोधन है।
4.	सूचना सुरक्षा नीतियों के लिए COBIT (DS5.2, DS5,3) और (DS5.2, ME2.5, ME2.7)	COBIT (जैसा कि उपभागों में उल्लेख किया गया है) सूचना सुरक्षा के लिए नीतियों और सूचना सुरक्षा के लिए नीतियों की समीक्षा के बारे में जानकारी प्रदान करता है।
5.	एनआईएसटी एसपी 800-100 सूचना सुरक्षा	सूचना सुरक्षा जटिलताओं और तकनीकों के लिए एक मैनुअल।
6.	सूचना प्रौद्योगिकी प्रशासन, जोखिम, नियंत्रण और आश्वासन अमल पर आरबीआई मास्टर निर्देश- आरबीआई/2023-24/107DoS.CO. CSITEG/SEC.7/31.01.015/2023-24	दिनांक 07 नवम्बर, 2023