आईटी बीसीपी/डीआर नीति

दस्तावेज़ कोड: हडको/ आईटी-नीतियाँ/2024/05

दस्तावेज़ वर्गीकरण: आंतरिक

(संस्करण 1.1)

हाउसिंग एंड अर्बन डेवलपमेंट लिमिटेड

कोर 7-ए, हडको भवन, इंडिया हैबीटेड सेंटर, लोधी रोड, नई दिल्ली 110003

वेबसाइट: www.hudco.org.in सीआईएन: एल74899 DL1970GOI005276

यह दस्तावेज़ केवल हाउसिंग एंड अर्बन डेवलपमेंट लिमिटेड (हडको) के आंतरिक उपयोग के लिए है और किसी अन्य व्यक्ति या संस्था द्वारा उपयोग के लिए अभिप्रेत नहीं है। इस नीति को बनाने के लिए अपनाई गई प्रक्रियाएँ हडको के आंतरिक नियंत्रणों, धोखाधड़ी का पता लगाने, या विधिक एवं विनियमों के अनुपालन का ऑडिट, वित्तीय विवरण समीक्षा, या परीक्षण नहीं हैं। हडको के वित्तीय विवरणों, आंतरिक नियंत्रणों या अनुपालन संबंधी मामलों के संबंध में कोई राय या आश्वासन नहीं दिया गया है।

संस्करण इतिहास

क्र . सं.	संस्करण सं.	प्रस्तुतकर्ता	जाँचकर्ता	समर्थनकर्ता	तिथि
1.	1.0	डेलॉइट कॉर्पोरेट फाइनेंस सेवाएं भारत	कार्यकारी निदेशक (आईटी)	हडको बोर्ड	08.01.2019
2.	1.1	एकेएस आईटी सर्विसेज प्रा. लिमिटेड	कार्यकारी निदेशक (आईटी)	हडको बोर्ड	16.12.2024

विषयसूची

1. परिचय 6
2. उद्देश्य 6
3. स्कोप 6
4. बीसीएम फ्रेमवर्क का उद्देश्य 7
5. अपवाद 7
6. व्यवसाय निरंतरता प्रबंध अवलोकन 7
7. व्यवसाय निरंतरता प्रबंध फ्रेमवर्क 7
8. जोखिम मूल्यांकन और नियंत्रण 8
9. व्यावसायिक प्रभाव विश्लेषण (बीआईए) 10
10. पुनर्प्राप्ति कौशलनीति विकसित करना 11
11. बीसीएम योजना विकास और प्रतिक्रिया 12
12. घटना रिपोर्टिंग 12
13. आपदा पुनर्प्राप्ति योजना....13
13.1 आपदा पुनर्प्राप्ति प्रबंधन....13
13.2 आपदा पुनर्प्राप्ति साइट के पास 13
14. बैकअप नीति 13
15. गंभीर सेवाएं स्थानांतरण योजना 14
16. आपातकाल प्रतिक्रिया योजना 14
17. असेंबली पॉइंट.... 14
18. जानकारी सुरक्षा 14
19. संचार और जनता जानकारी योजना 14
20. व्यापार निरंतरता प्रबंध संरचना 15
21. क्षति आकलन टीम की भूमिकाएं और जिम्मेदारियां 15
22. आपातकाल प्रतिक्रिया टीम की भूमिकाएँ और जिम्मेदारियां 16
22.1 मुख्य आपातकाल समन्वयक 16
22.2 आपातकाल प्रतिक्रिया स्टाफ 16
23. आपातकालीन स्थितियों पर प्रतिक्रिया देने के लिए बीसीपी टीमों के लिए दिशानिर्देश.... 17
23.1 अग्नि सुरक्षा दिशानिर्देश 17
23.2 आग लगने की स्थिति में....17
23.3 आग लगने के बाद 18
23.4 मानव संसाधन जिम्मेदारियाँ 18
23.5 फायर ड्रिल 18

23.6 भूकंप 18
23.7 बिजली कटौती 19
23.8 चिकित्सा आपातकाल 19
23.9 बम ख़तरा प्रक्रियाएँ 20
23.10 विकलांग व्यक्तियों के लिए आपातकाल निकास 20
24. घटना रिपोर्टिंग संपर्क 22
25. आपातकाल सेवाएँ 22
26. अभ्यास और सत्यापन अवधारणा 23
26.1 अभ्यास के उद्देश्य 23
26.2 अभ्यास दायरा 23
26.3 अभ्यास अनुसूची 23
26.4 अभ्यास पद्धति 23
26.5 घोषित और अघोषित अभ्यास 23
26.6 मूल्यांकन का अभ्यास 23
26.7 अभ्यास के बाद रिपोर्टिंग 24
26.8 परिवर्तन प्रबंधन प्रक्रिया (सीखे गए सबक के जवाब में) 24
27. प्रशिक्षण और जागरूकता 24
28. रखरखाव प्रोटोकॉल की योजना 25
28.1 टीमें और जिम्मेदारियाँ 25
28.2 योजना को अद्यतन करने के लिए परिवर्तन नियंत्रण प्रक्रिया 25
28.3 रखरखाव अनुसूची 25
29. घटना प्रतिक्रिया योजना 26
29.1 साइबर घटना प्रतिक्रिया के लक्ष्य 26
29.2 उद्देश्य और स्कोप 26
29.3 घटना प्रतिक्रिया जीवन चक्र प्रक्रिया 26
29.4 घटना प्रतिक्रिया टीम (आईआरटी) 27
29.5 साइबर घटना प्रतिक्रिया टीम (आईआरटी): 27
29.6 घटना प्रतिक्रिया प्रक्रिया विवरण 28
29.7 तैयारी 29
29.8 घटना घटित होना और जागरूकता 29
29.9 घटना प्रतिक्रिया उपकरण 29
29.10 घटना की पहचान 30
29.11 रोकथाम 30

29.12 उन्मूलन 30
29.13 रिकवरी 31
29.14 घटना के बाद का विश्लेषण 31
30 एजेंसियों को घटनाओं का प्रकार और विवरण सूचित करना 31
30.1 सीईआटी - आईएन को घटनाओं की रिपोर्ट.....31
30.2 जानकारी रिकॉर्डिंग 33

परिशिष्ट- ए 35
परिशिष्ट- बी 36
परिशिष्ट- सी 40

1. परिचय

व्यावसायिक निरंतरता योजना (बीसीपी) एक संगठन की तैयारी प्रक्रिया है जो यह सुनिश्चित करती है कि असाधारण परिस्थितियों में भी महत्वपूर्ण व्यावसायिक कार्य उपलब्ध रहें। प्रभावी बीसीपी दैनिक गतिविधियों के लिए सेवा स्तर, स्थिरता और पुनर्प्राप्ति क्षमता बनाए रखने हेतु एक रोडमैप विकसित करती है। बीसीपी को कभी-कभी आपदा पुनर्प्राप्ति के साथ जोड़ दिया जाता है; हालाँकि, आपदा पुनर्प्राप्ति बीसीपी का एक उपसमूह है क्योंकि सभी व्यावसायिक व्यवधानों को आपदाओं की श्रेणी में नहीं रखा जाएगा।

व्यवसाय निरंतरता प्रबंधन ('बीसीएम') एक समग्र प्रबंधन प्रक्रिया है जो किसी संगठन के लिए खतरा पैदा करने वाले संभावित प्रभावों की पहचान करती है और एक प्रभावी प्रतिक्रिया के लिए लचीलापन और क्षमता निर्माण हेतु एक ढांचा प्रदान करती है जो इसके प्रमुख शेयरधारकों, प्रतिष्ठा, ब्रांड और मूल्य सृजन गतिविधियों के हितों की रक्षा करती है।

एक उचित रूप से डिज़ाइन, कार्यान्वित और अनुरक्षित बीसीएम कार्यक्रम के माध्यम से, हडको किसी भी आपदा या संकट की स्थिति में प्रतिक्रिया देने के लिए तैयार रहेगा। बीसीएम कार्यक्रम के विस्तृत तत्व व्यवसाय को किसी भी प्रकार के व्यावसायिक व्यवधान की स्थिति में अपने महत्वपूर्ण कार्यों को अधिक कुशलता से पुनः प्राप्त करने में मदद करते हैं। चूँकि आईटी अनुप्रयोग केंद्रीकृत वातावरण में तैनात किए जाते हैं, इसलिए नीति का क्रियान्वयन कॉर्पोरेट कार्यालय स्तर पर किया जाएगा।

2. उद्देश्य

व्यवसाय निरंतरता नीति (बीसीपी) का उद्देश्य यह सुनिश्चित करना है कि हडको किसी आपदा या व्यवधान के दौरान और उसके बाद भी अपने आवश्यक कार्य जारी रख सके। इसके उद्देश्य को रेखांकित करने वाले प्रमुख बिंदु नीचे दिए गए हैं:

1. **डाउनटाइम न्यूनतम करें:** आपात स्थिति में व्यवधान के दौरान न्यूनतम लागत पर महत्वपूर्ण व्यावसायिक संचालनों की निरंतरता सुनिश्चित करें।
2. **जोखिम न्यूनीकरण:** संभावित जोखिमों की पहचान करें और संचालन पर उनके प्रभाव को कम करने के लिए कौशलनीति विकसित करें।
3. **संसाधन उपलब्धता:** संचालन को बनाए रखने के लिए आवश्यक संसाधनों (कार्मिक, प्रौद्योगिकी, डेटा और सुविधाएं) की उपलब्धता सुनिश्चित करें।
4. **संपत्तियों की सुरक्षा:** भौतिक, डिजिटल और बौद्धिक संपत्तियों को संभावित खतरों से सुरक्षित रखें।
5. **सुरक्षा सुनिश्चित करें:** स्पष्ट सुरक्षा प्रोटोकॉल लागू करके कर्मचारियों, ग्राहकों और हितधारकों की सुरक्षा करें।
6. **विनियामक अनुपालन:** व्यवसाय निरंतरता और आपदा पुनर्प्राप्ति से संबंधित कानूनी और विनियामक आवश्यकताओं को पूरा करना।
7. **ग्राहक विश्वास बनाए रखें:** ग्राहकों के प्रति विश्वसनीयता और लचीलापन प्रदर्शित करें, जिससे विश्वास और वफादारी बनी रहे।
8. **प्रतिष्ठा की सुरक्षा:** संगठन की सार्वजनिक छवि और विश्वसनीयता पर व्यवधानों के प्रभाव को कम करना।
9. **पुनर्प्राप्ति को सुगम बनाना:** किसी घटना के बाद सामान्य परिचालन को शीघ्रता एवं कुशलता से बहाल करने के लिए स्पष्ट रोडमैप प्रदान करना।
10. **सक्षम अनुकूलनशीलता:** अप्रत्याशित घटनाओं से अनुकूलन करने और उनसे उबरने के लिए संगठनात्मक लचीलापन बनाएं।

व्यवधानों के लिए सक्रिय रूप से योजना बनाकर, बीसीपी यह सुनिश्चित करता है कि संगठन आवश्यक सेवाओं को बनाए रखते हुए और जोखिमों को कम करते हुए संकट से निपटने के लिए तैयार है।

3. स्कोप

यह नीति पूर्णकालिक एवं अंशकालिक सहयोगियों, ठेकेदारों, विक्रेताओं और बाहरी सलाहकारों सहित सभी हडको प्रबंधन पर लागू है।

4. बीसीएम फ्रेमवर्क का उद्देश्य

- वित्तीय नुकसान को कम करना ।
- आईटी संसाधनों की सुरक्षा सुनिश्चित करना ।
- आपदा के दौरान कर्मचारियों, ग्राहकों और प्रतिपक्षों को सेवा प्रदान करना जारी रखना।
- कौशलनीतिक योजना की प्रतिष्ठा, संचालन, आय, तरलता, ऋण गुणवत्ता, बाजार स्थिति और संस्था की लागू विधिक और विनियमों के अनुपालन में बने रहने की क्षमता पर व्यवधानों के नकारात्मक प्रभाव को कम करना।

5. अपवाद

ऐसे कई उदाहरण हो सकते हैं जहाँ व्यावसायिक निरंतरता योजना नीति के विपरीत कार्य करने की 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 कार्यकारी निदेशक (आईटी) द्वारा अनुमोदित किया जाना आवश्यक है। सभी अनुमोदित अपवादों की कम से कम वार्षिक या आवश्यकतानुसार समीक्षा की जानी चाहिए। व्याख्या से संबंधित किसी भी मुद्दे को सक्षम प्राधिकारी द्वारा अनुमोदित किया जाना चाहिए।

6. व्यवसाय निरंतरता प्रबंधन अवलोकन

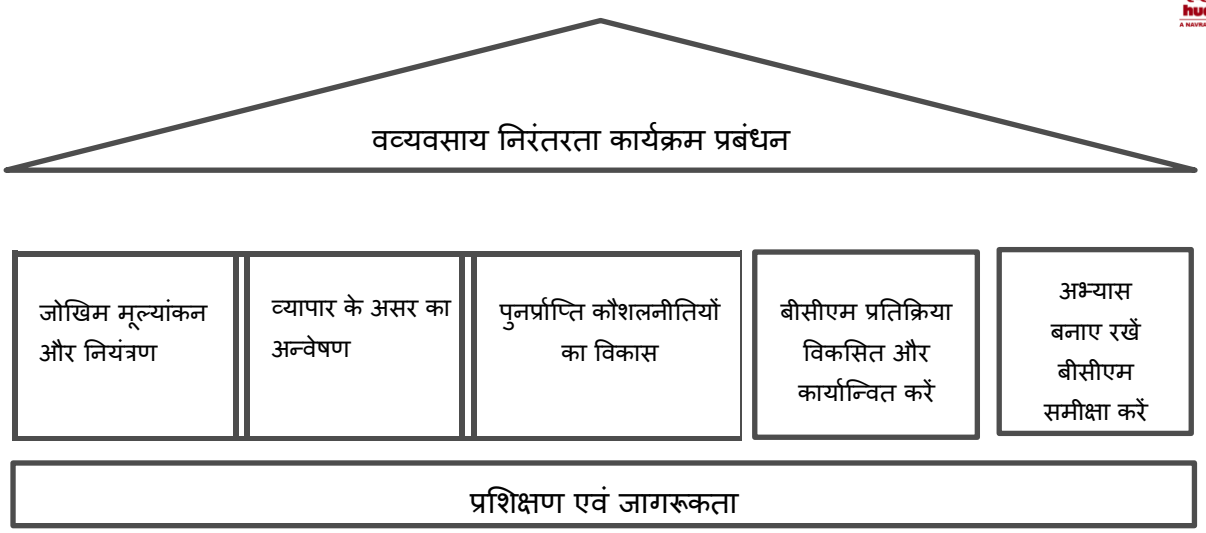
व्यवसाय निरंतरता प्रबंधन के लिए कौशलनीतियों, योजनाओं, संसाधनों और कार्यों के विकास और कार्यान्वयन की आवश्यकता होती है, ताकि किसी महत्वपूर्ण, अप्रिय, संकट की स्थिति में महत्वपूर्ण उद्देश्यों की निरंतर उपलब्धि सुनिश्चित की जा सके।

बीसीएम पर केंद्रित है

- संगठनों के भीतर निर्भरताओं/कमजोरियों की पहचान करना, विशेष रूप से वे जो मूल्य सृजन की अंतर्निहित प्रक्रियाओं से जुड़ी हैं। समय के साथ उनकी अनुपलब्धता का संगठन पर पड़ने वाले प्रभाव को समझना।
- आपदा की स्थिति में समग्र मूल्य सृजन पर प्रभाव को न्यूनतम करने के लिए प्रक्रिया की पहचान करना।

7. व्यवसाय निरंतरता प्रबंधन फ्रेमवर्क

हडको को किसी संकट के लिए तैयार करने में एक ऐसा ढाँचा तैयार करना शामिल है जो व्यावसायिक व्यवधानों के प्रति लचीला हो और साथ ही विभिन्न स्तरों की रुकावटों और रुकावटों का प्रभावी ढंग से सामना करने में सक्षम हो। तैयारी प्रक्रिया के चरणों में जोखिम मूल्यांकन और नियंत्रण, व्यावसायिक प्रभावों का विश्लेषण, पुनर्प्राप्ति कौशलनीतियों का विकास, योजना विकास और कार्यान्वयन, अभ्यास और प्रशिक्षण शामिल हैं। विभागीय मानकों का पालन करने से हडको किसी संकट के लिए इस तरह तैयार होगा कि वह कॉर्पोरेट नीति के अनुरूप हो और उद्योग द्वारा पसंद की जाने वाली व्यावसायिक निरंतरता प्रबंधन प्रचलन का पालन करें।



8. जोखिम मूल्यांकन और नियंत्रण

जोखिम विश्लेषण से उन परिस्थितियों के स्रोतों का निर्धारण होता है जो महत्वपूर्ण संसाधनों की हानि की स्थिति में हडको और इसकी सुविधाओं पर प्रतिकूल प्रभाव डाल सकती हैं, ऐसी परिस्थितियों से होने वाली क्षति और संभावित हानि के प्रभावों को रोकने और न्यूनतम करने के लिए आवश्यक नियंत्रणों का निर्धारण होता है।

व्यावसायिक निरंतरता योजना टीम द्वारा प्रतिवर्ष (या संगठन या व्यावसायिक परिवेश में होने वाले परिवर्तनों के अनुरूप) एक जोखिम विश्लेषण किया जाएगा। जोखिम विश्लेषण पूरा करने के लिए आवश्यक आंतरिक और बाह्य संसाधन जुटाना संबंधित समन्वयकों की ज़िम्मेदारी है। आईटी अवसंरचना और अनुप्रयोगों सहित, व्यावसायिक क्षेत्र के संचालन के सभी पहलुओं के लिए जोखिम विश्लेषण किया जाएगा।

निम्नलिखित विभागीय ट्रिगर्स से यह संकेत मिलेगा कि वार्षिक अनुसूची की तुलना में जोखिम का पुनर्मूल्यांकन आवश्यक है:-

- नये भवन का अधिग्रहण।
- भौतिक परिवेश में परिवर्तन (अर्थात् भवनों का निर्माण, शहर के खतरे, आदि)।
- नये उत्पाद या व्यावसायिक साझेदार संबंध।
- नेटवर्क आर्किटेक्चर में परिवर्तन।
- डेटा सेंटर के स्थान और/या डिज़ाइन में परिवर्तन।
- महत्वपूर्ण नए नियम ।
- महत्वपूर्ण प्रक्रिया परिवर्तन ।

प्रत्येक संभावित जोखिम की संभावना और उसके संभावित प्रभाव का आकलन करने के लिए हडको में एक सामान्य जोखिम विश्लेषण पद्धति का उपयोग किया जाएगा। यह पद्धति सूचना एकत्रीकरण, संभावना और गंभीरता के मूल्यांकन, एक सतत मूल्यांकन प्रक्रिया, भौतिक, सूचना सुरक्षा, कानूनी और नियामक मुद्दों की पहचान, और संभावित जोखिम से जुड़े लागत और लाभों के विश्लेषण के लिए एक सामान्य विधि प्रदान करेगी।

कम से कम, आंतरिक और बाहरी दोनों स्रोतों से पर्यावरणीय, तकनीकी, संचालनात्मक, राजनीतिक, विधिक और सुरक्षा जोखिमों की पहचान की जाएगी। पहचाने गए प्रत्येक जोखिम के लिए, घटित होने की संभावना और संभावित नुकसान का आकलन किया जाएगा। जोखिम और संभावित नुकसान के प्रभाव को रोकने और/या कम करने के लिए मौजूदा नियंत्रणों और सुरक्षा उपायों की पहचान की जाएगी और उनकी प्रभावशीलता का आकलन किया जाएगा।

विशिष्ट नियंत्रणों की पहचान और मूल्यांकन किया जाएगा, जिनमें निम्नलिखित शामिल हो सकते हैं, लेकिन इन्हीं तक सीमित नहीं होंगे:

- भौतिक स्थान

- भौतिक अवसंरचना डिजाइन
- भवन सुरक्षा और एक्सेस नियंत्रण
- कार्मिक प्रक्रियाएँ
- तृतीय-पक्ष अनुबंध
- सूचना सुरक्षा (जैसे डेटा सेंटर, नेटवर्क, हार्डवेयर, ऑपरेटिंग सिस्टम, एप्लिकेशन, डेटाबेस स्तर की सुरक्षा)
- सूचना बैकअप और सुरक्षा
- निवारक रखरखाव और उपकरण नियोजन
- अनावश्यक सेवाएँ (बिजली, एयर कंडीशनिंग, पानी, संचार, उपकरण प्रतिस्थापन और पुर्जे)

नियंत्रण मुख्यतः निवारक प्रकृति के होने चाहिए। जहाँ निवारक नियंत्रण विकल्प उपलब्ध न हों, वहाँ जासूसी और सुधारात्मक नियंत्रणों के बीच उचित संतुलन लागू किया जाएगा। व्यवसाय क्षेत्र का प्रमुख यह निर्धारित करेगा कि जोखिमों से बचना है, उन्हें स्थानांतरित करना है और/या स्वीकार करना है, और नियंत्रणों में प्रस्तावित निवेश को अनुमोदित करेगा।

बीसीएम लीडर उन जोखिम हस्तांतरण और स्वीकृति तकनीकों से जुड़े विवादों का समाधान करेगा जो लागू तो हैं, लेकिन किसी अन्य व्यावसायिक क्षेत्र की ज़रूरतों और प्रभावों के साथ टकराव करते हैं।

जोखिम मूल्यांकन के लिए निम्नलिखित विभाग निम्नलिखित खतरों पर विचार करते हैं:

प्राकृतिक खतरों	**आकस्मिक खतरों**
भूकंप	आग
चक्रवात	उपकरण/आईटी हार्डवेयर विफलता
बाढ़	भवन/संरचना का ढहना
महामारी का प्रकोप	
जानबूझकर की गई हरकतें	बुनियादी ढाँचे से संबंधित खतरे
बम की धमकी	बिजली व्यवधान
नागरिक विकार	दूरसंचार / इंटरनेट व्यवधान
सेवा से इनकार	पानी हानि
क्रूर बल हमला	प्लेटफ़ॉर्म/वीएम/एप्लिकेशन का कम प्रदर्शन
मैलवेयर	डेटा पुनर्स्थापित नहीं किया जा सकता
दुश्मन आक्रमण करना, युद्ध	
तोड़-फोड़	
अपराध	
बाहरी/आंतरिक हमलावर द्वारा पैच न किए गए एप्लिकेशन/सिस्टम पर हमला	
बाहरी/आंतरिक हमलावर द्वारा असुरक्षित	
बाहरी/आंतरिक हमलावर द्वारा पुराने प्लेटफ़ॉर्म पर हमला	
विशेषाधिकार प्राप्त एक्सेस	
भौतिक सुरक्षा उल्लंघन	

9. व्यावसायिक प्रभाव विश्लेषण (बीआईए)

व्यवसाय प्रभाव विश्लेषण एक प्रबंधन स्तर का विश्लेषण है जो कंपनी के संसाधनों, संगठन की प्रतिष्ठा को खोने के प्रभावों की पहचान करता है; समय के साथ संसाधन हानि और बढ़ती हानि के प्रभाव को मापता है ताकि वरिष्ठ प्रबंधन को विश्वसनीय डेटा प्रदान किया जा सके जिसके आधार पर जोखिम न्यूनीकरण और निरंतरता योजना पर निर्णय लिया जा सके।

व्यावसायिक प्रभाव विश्लेषण उन व्यवधानों और आपदा परिदृश्यों से उत्पन्न प्रभावों की पहचान करता है जो संगठन को प्रभावित कर सकते हैं, और उन तकनीकों की पहचान करता है जिनका उपयोग ऐसे प्रभावों को मापने और वर्गीकृत करने के लिए किया जा सकता है। बीआईए का उपयोग समय-महत्वपूर्ण कार्यों, पुनर्प्राप्ति प्राथमिकताओं, संसाधनों और अंतर-निर्भरताओं की पहचान करने के लिए किया जाता है ताकि पुनर्प्राप्ति समय उद्देश्य (RTO), पुनर्प्राप्ति बिंदु उद्देश्य (RPO) और व्यवधान की अधिकतम सहनीय अवधि (MTPD) निर्धारित की जा सके।

हडको को एक डीआर साइट की योजना बनानी और उसे लागू करना होगा जहाँ सभी चिन्हित सर्वर/ एप्लिकेशन होस्ट किए जाने चाहिए। हडको को प्राप्त आरपीओ/आरटीओ के साथ डीआर अभ्यास गतिविधियों का रिकॉर्ड दर्ज करना होगा। डीआर अभ्यास रिपोर्ट बोर्ड की आईटी कौशलनीति समिति के समक्ष प्रस्तुत की जाएगी।

क्र.सं.	व्यावसायिक प्रक्रिया और सेवा	सिस्टम एप्लिकेशन	मिनटों, घंटों, दिनों, हफ्तों में अधिकतम सहनीय डाउनटाइम	वसूली समय उद्देश्य (आरटीओ)	पुनर्प्राप्ति बिंदु उद्देश्य (आरपीओ)

डी.आर. ड्रिल के दौरान देखी गई किसी भी बड़ी समस्या का समाधान किया जाएगा तथा अगले चक्र से पहले ड्रिल के सफल संचालन को सुनिश्चित करने के लिए पुनः परीक्षण किया जाएगा।

डी.आर. परीक्षण में डी.आर./वैकल्पिक साइट पर स्विच करना और इस प्रकार इसे पर्याप्त रूप से लंबी अवधि के लिए प्राथमिक साइट के रूप में उपयोग करना शामिल होगा, जहां कम से कम एक पूर्ण कार्य दिवस (दिन के आरंभ से लेकर दिन के अंत तक के संचालन सहित) के सामान्य व्यावसायिक संचालन को कवर किया जाता है।

हडको संभावित प्रकार की आकस्मिकताओं के लिए विभिन्न परिदृश्यों के तहत बीसीपी/डीआर का नियमित रूप से परीक्षण करेगा, ताकि यह सुनिश्चित किया जा सके कि यह अद्यतन और प्रभावी है।

हडको यह सुनिश्चित करेगा कि आपातकालीन स्थिति में किसी भी रिकवरी ऑपरेशन के लिए डी.आर. संरचना और प्रक्रियाएं मजबूत हों तथा परिभाषित आर.टी.ओ. और आर.पी.ओ. को पूरा करें।

हडको, विक्रेताओं और साझेदारों सहित, महत्वपूर्ण अंतर्संबंधित प्रणालियों और नेटवर्कों में बीसीपी और डीआर क्षमताओं को सुनिश्चित करेगा। हडको, हडको के आरटीओ के अनुरूप सहयोगात्मक और समन्वित लचीलापन परीक्षण के माध्यम से प्रदर्शित तत्परता सुनिश्चित करेगा।

10. पुनर्प्राप्ति कौशलनीति विकसित करना

पहचाने गए जोखिमों और व्यवधानों के संभावित व्यावसायिक प्रभावों को कम करने के लिए पुनर्प्राप्ति कौशलनीतियाँ विकसित की जाती हैं। कौशलनीतियाँ का चयन और कार्यान्वयन व्यावसायिक प्राथमिकताओं और उद्देश्यों के अनुसार किया जाता है।

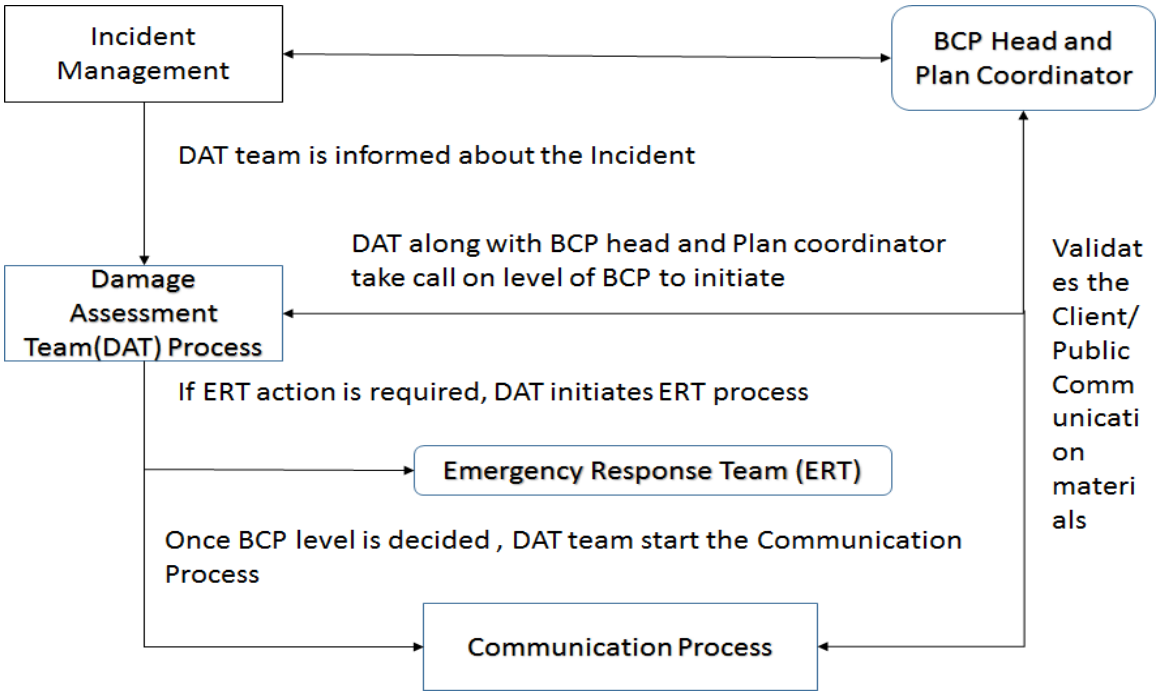
नीचे दी गई तालिका में धारणा और बीसीपी गतिविधि के साथ-साथ बीसीपी के परिदृश्यों/स्तरों का संक्षिप्त विवरण दिया गया है।

आपदा स्तर	आपदा विवरण	बीसीपी गतिविधि
एल1- ए	जोखिम मूल्यांकन (आरए) अनुभाग में सूचीबद्ध खतरों या अज्ञात खतरे के कारण हडको मुख्यालय में संचालन सुविधा उपलब्ध नहीं है।	यदि सुविधा को इतनी क्षति पहुँचती है कि वह महीनों तक अनुपलब्ध हो जाती है, तो महत्वपूर्ण प्रक्रियाओं/गतिविधियों की देखभाल करने वाले सभी कर्मचारियों को घर/वैकल्पिक स्थान से काम करने और मूल सुविधा बहाल होने तक वहीं से काम करने की अनुमति दी जाएगी। सुविधा टीम बाहरी विक्रेताओं (यदि आवश्यक हो) के साथ मिलकर मूल सुविधा / आईटी अवसंरचना को बहाल करने की दिशा में काम करती है। एक बार सुविधा/आईटी अवसंरचना बहाल हो जाने पर, बीसीपी समन्वयक और बीसीपी प्रमुख को इसके बारे में सूचित किया जाता है। सभी कर्मचारियों को बहाली के बारे में सूचित कर दिया गया है और वे हडको मुख्यालय से काम शुरू कर देंगे तथा सामान्य संचालन फिर से शुरू कर देंगे।
एल1- बी	हडको मुख्यालय का संचालन उपलब्ध है, तथापि, बिजली/ दूरसंचार/डेटा व्यवधान के कारण इसका संचालन अक्रियाशील हो गया है।	हडको मुख्यालय के प्रत्येक कार्मिकों के पास लैपटॉप होंगे तथा वैकल्पिक स्थान पर स्थित संसाधन संचालन का कार्यभार संभालेंगे, ताकि वे अपने घर से या वैकल्पिक स्थान से काम कर सकें।
एल1- सी	सामूहिक इस्तीफे/महामारी के कारण हडको मुख्यालय के कार्मिक उपलब्ध नहीं हैं।	हडको मुख्यालय के कार्मिकों की अनुपलब्धता के दौरान, वैकल्पिक स्थान पर स्थित संसाधन संचालन का कार्यभार संभालेंगे। वैकल्पिक स्थान के संसाधन हडको मुख्यालय के संसाधनों की दोगुनी जिम्मेदारी और कार्यभार संभालेंगे।

11. बीसीएम योजना विकास और प्रतिक्रिया

व्यवसाय निरंतरता योजनाओं को व्यवसाय की आवश्यकताओं को पूरा करने वाली पुनर्प्राप्ति कौशलनीतियों के आधार पर दस्तावेजित और कार्यान्वित किया जाता है।

कौशलनीति और सक्रियण मानदंड



12. घटना रिपोर्टिंग

किसी घटना को पहली बार नोटिस करने पर, जिससे संचालन में व्यवधान उत्पन्न हो सकता है, घटना प्रबंधन टीम तुरंत क्षति आकलन समन्वयक, बीसीपी समन्वयक और बीसीपी प्रमुख को सूचित करेगी।

सामान्य निकास प्रक्रिया

- भवन में रहने वालों को भवन के अग्नि अलार्म की ध्वनि या भवन के आपातकालीन कर्मचारियों के मौखिक निर्देश द्वारा खाली करने की सूचना दी जाएगी।
- यदि अग्नि अलार्म सक्रिय हो जाए, या भवन के आपातकालीन कर्मचारियों द्वारा ऐसा करने का निर्देश दिया जाए, तो सभी निवासियों को तुरंत भवन छोड़ देना चाहिए।
- भवन के आपातकालीन कर्मचारी यथासंभव निकासी में मार्गदर्शन और सहायता करेंगे।
- सभी निवासियों को निकटतम सुरक्षित निकास द्वार या निकास द्वार से इमारत से बाहर निकलना चाहिए। आपातकालीन निकासी में लिफ्ट का उपयोग कभी नहीं करना चाहिए।
- यदि निकटतम निकास धुएं, आग या अन्य खतरों से अवरुद्ध है, तो वैकल्पिक निकास या निकास सीढ़ी की ओर बढ़ें।
- सीढ़ियों से उतरते समय ऊँची एड़ी के जूते उतार दें और रेलिंग को पकड़ लें। सीढ़ियों पर यातायात के प्रवाह में दूसरों के आने-जाने के लिए पर्याप्त जगह छोड़ें।

- बाहर निकलने के बाद सभी निवासियों को भवन के समीप स्थित पार्किंग स्थल में स्थित सभा क्षेत्र में चले जाना चाहिए।
- आपातकालीन स्टाफ सदस्यों को यह सुनिश्चित करना चाहिए कि यदि आवश्यक हो तो अग्निशमन/पुलिस/ एम्बुलेंस विभाग आदि को फोन करके उचित सहायता बुलाई गई है।
- एक बार एकत्र हो जाने पर, आपातकालीन कर्मचारी सभी निवासियों का लेखा-जोखा रखेंगे, ताकि यदि कोई लापता हो या संभवतः अभी भी इमारत के अंदर हो तो आपातकालीन सेवाओं को सूचित किया जा सके।
- भवन का आपातकालीन स्टाफ आने वाले आपातकालीन कर्मियों को भवन में आपातकाल के बारे में जानकारी देगा, जिसमें खतरों का स्थान और ज्ञात कोई भी समस्या शामिल होगी।
- आपातकालीन कर्मियों द्वारा अनुमति दिए जाने तक भवन में रहने वालों को पुनः प्रवेश नहीं करना चाहिए।

13. आपदा पुनर्प्राप्ति योजना

131 आपदा पुनर्प्राप्ति प्रबंधन

- महत्वपूर्ण इन्फ्रास्ट्रक्चर और फेलओवर क्षमताओं के साथ प्राथमिक डेटा सेंटर को प्रतिबिंबित करने के लिए एक ऑफ-साइट स्थान स्थापित करें।
- हडको को न्यूनतम आरटीओ (जैसा कि हुडको के आईटीएससी द्वारा अनुमोदित है) और महत्वपूर्ण सूचना प्रणालियों के लिए लगभग शून्य आरपीओ प्राप्त करने को प्राथमिकता देनी चाहिए।
- गैर-शून्य आरपीओ के परिदृश्य में, हुडको के पास वैकल्पिक स्थान से संचालन पुनः शुरू करते समय डेटा के समाधान के लिए एक प्रलेखित कार्यप्रणाली होगी।
- हडको यह सुनिश्चित करेगा कि डीसी और डीआर पर सूचना प्रणालियों और तैनात सुरक्षा पैचों का विन्यास समान हो।

132 आपदा पुनर्प्राप्ति साइट के पास:

- महत्वपूर्ण इन्फ्रास्ट्रक्चर और फेलओवर क्षमताओं के साथ प्राथमिक डेटा सेंटर को प्रतिबिंबित करने के लिए एक ऑफ-साइट स्थान स्थापित करें।
- आपात स्थिति के दौरान न्यूनतम डाउनटाइम और त्वरित सेवा परिवर्तन सुनिश्चित करें।
- आईटी कौशलनीति योजना में आवश्यक सेवाओं (जैसे, पेरोल, ऋण प्रसंस्करण, ईआरपी) की पहचान करें और उन्हें प्राथमिकता दें।
- सुनिश्चित करें कि ये सेवाएं आपदा पुनर्प्राप्ति स्थल पर चालू हों।

14. बैकअप नीति

बैकअप नीति के अनुसार, निम्नलिखित बताया गया है-

- सभी निर्धारित बैकअप की आवृत्ति, अनुप्रयोगों की गंभीरता और व्यावसायिक निरंतरता योजना में उल्लिखित उनके निर्धारित पुनर्प्राप्ति बिंदु उद्देश्यों (आरपीओ) के आधार पर ली जानी चाहिए। बैकअप की आवृत्ति पूरी तरह से बैकअप किए जाने वाले डेटा और अनुप्रयोग की संबंधित गंभीरता पर निर्भर करती है।
- आईटी विभाग बैकअप प्रक्रिया स्थापित करने के लिए जिम्मेदार होगा।
- पूर्ण डेटाबेस और एप्लिकेशन बैकअप प्रतिदिन लिया जाएगा।
- हडको डेटा का बैकअप लेगा और उसकी उपयोगिता की जाँच के लिए समय-समय पर बैकअप डेटा को पुनर्स्थापित करेगा। ऐसे बैकअप डेटा की अखंडता को बनाए रखने के साथ-साथ उसे अनधिकृत एक्सेस से भी सुरक्षित रखा जाएगा।

15. गंभीर सेवाएँ स्थानांतरण योजना

व्यावसायिक प्रभाव विश्लेषण से पहचानी गई सभी प्रमुख प्रक्रियाएँ इस गतिविधि के प्रत्यक्ष दायरे में होंगी। हडको मुख्यालय में सभी महत्वपूर्ण व्यावसायिक और सहायक सेवाएँ, वैकल्पिक स्थान पर स्थित कार्य केंद्र में स्थानांतरित कर दी जाएँगी।

सूचना प्रौद्योगिकी विभाग करेगा:

- विकास गतिविधि का नेतृत्व करने के लिए आवश्यक महत्वपूर्ण संसाधनों और महत्वपूर्ण कर्मियों की पहचान करें।
- कार्य के लिए महत्वपूर्ण के रूप में चुने गए कार्मिकों को आपदा की स्थिति में कार्य करने के तरीके के बारे में प्रशिक्षित किया जाएगा।
- कार्मिकों से नियमित स्थिति की जानकारी प्राप्त करें, ग्राहक(ओं) से संवाद करें और उन्हें व्यवसाय की निरंतरता का आश्वासन दें।

16. आपातकाल प्रतिक्रिया योजना

यह प्रक्रियाओं का एक मानक समूह है जो जीवन की सुरक्षा के लिए प्रारंभिक प्रतिक्रिया और सभी कर्मियों की सुरक्षा सुनिश्चित करने के लिए गतिविधियों के साथ-साथ किसी आपात स्थिति के प्रभाव को कम करने के लिए आवश्यक गतिविधियों और आपातकालीन स्थिति को न्यूनतम करने या नियंत्रित करने के लिए आपातकालीन कर्मियों के साथ काम करने को संबोधित करता है।

हडको मुख्यालय के प्रशासनिक विभाग में सामान्य उपयोग के लिए एक आपातकालीन किट रखेगा। आपातकालीन निकासी की स्थिति में, मुख्यालय के कार्मिक इस किट को निकासी क्षेत्र में ले जाएँगे। किट में शामिल हैं:

- इस आपातकालीन योजना (बीसीपी का आपातकालीन प्रतिक्रिया योजना अनुभाग) की एक प्रति, वर्तमान कार्मिक रोस्टर के साथ, निकासी के बाद भवन कर्मियों के लिए प्राथमिक चिकित्सा आपूर्ति का लेखा-जोखा रखने में उपयोग की जाएगी। कुछ आपात स्थितियों में, कार्मिकों को गैर-जीवन-खतरनाक चोटों वाले व्यक्तियों को प्राथमिक उपचार प्रदान करना पड़ सकता है।
- फ्लैशलाइट और अतिरिक्त बैटरी।
- छोटी आपातकालीन जल एवं खाद्य आपूर्ति।
- सभी कार्मिकों के प्रमुख पारिवारिक सदस्यों के फोन नंबर सहित आवश्यक फोन नंबरों की सूची।

17. असेंबली पॉइंट

- जहां परिसर को खाली करने की आवश्यकता होती है, आपातकालीन प्रतिक्रिया योजना निकासी स्थल की पहचान करती है:
- हडको मुख्यालय के सामने, कोर-7ए गेट ।

18. जानकारी सुरक्षा

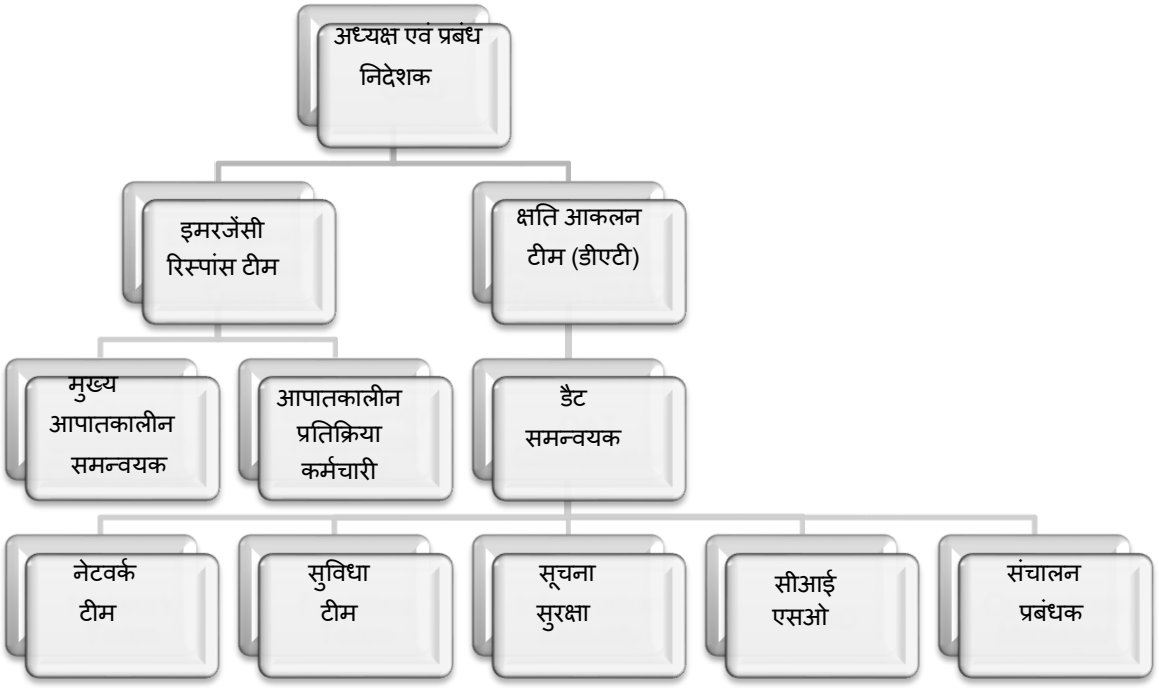
- किसी आपदा में, सारा ध्यान महत्वपूर्ण व्यावसायिक प्रक्रियाओं को फिर से चालू करने पर होना चाहिए। चाहे आपदा प्राकृतिक हो या मानव निर्मित, इसका उद्देश्य व्यावसायिक संचालन को यथाशीघ्र बहाल करना, कर्मचारियों को काम पर वापस लाना और महंगे डाउनटाइम से बचना है।
- इस परिदृश्य में, रिकवरी स्थिति के ऊपर सुरक्षा उल्लंघन का खतरा आम तौर पर सूचना सुरक्षा अक्सर विचार की सूची में बहुत नीचे होती है, लेकिन हडको समझता है कि जो कंपनियां अपने आपदा रिकवरी/व्यावसायिक निरंतरता योजनाओं में डेटा सुरक्षा प्रावधानों की अनदेखी करती हैं, उन्हें दोहरी समस्या का सामना करना पड़ सकता है,
- हडको यह सुनिश्चित करने के लिए प्रतिबद्ध है कि पुनर्प्राप्ति स्थिति में सुरक्षा नीतियों को बनाए रखा जाए।

19. संचार और जनता जानकारी योजना

- आपातकालीन घटना पूर्व चेतावनी के साथ या बिना पूर्व सूचना के घटित हो सकती है। दोनों ही स्थितियों में संचार प्रक्रिया एक जैसी होगी। कर्मचारियों को सूचित करने का तरीका इस बात पर निर्भर करता है कि आपातकाल का प्रकार क्या है और यह कि आपातस्थिति सामान्य व्यावसायिक घंटों के दौरान हुई है या उसके बाद। संचार फ़ोन, ईमेल, मौखिक या मोबाइल फ़ोन के माध्यम से किया जाएगा।

- प्रथम उत्तरदाता को बीसीपी प्रमुख और बीसीपी समन्वयक को सूचित करना होगा। सभी ज्ञात जानकारी बीसीपी समन्वयक और बीसीपी प्रमुख को प्रेषित की जाएगी।
- बीसीपी समन्वयक ईआरटी टीम के अनुसार संबंधित कार्मिकों से संपर्क करेगा।
- बीसीपी के सक्रिय होने पर, प्रभावित साइट (अर्थात आपदा से प्रभावित साइट) के टीम लीड अपने टीम सदस्यों को सूचित करेंगे।
- संचार समन्वयक को यह सुनिश्चित करना होगा कि सभी कर्मचारियों को सूचित कर दिया गया है कि वे जानकारी जारी न करें और अनुरोधों को संगठन के प्रवक्ता के पास भेज दें।
- आवश्यकतानुसार उपयुक्त मीडिया का उपयोग करके विज्ञापन दें।
- आवश्यकतानुसार ग्राहकों से संपर्क करें और उन्हें महत्वपूर्ण जानकारी प्रदान करें जैसे कि आपदा की प्रकृति, घोषित बीसीपी का स्तर अर्थात आपदा स्तर एल1 तथा सेवा वितरण पर संभावित प्रभाव आदि।

20. व्यापार निरंतरता प्रबंध संरचना



21. क्षति आकलन टीम की भूमिकाएं और जिम्मेदारियां

- अनियंत्रित/नए खतरों के कारण वर्तमान क्षति का आकलन करना।
- आपातकालीन प्रतिक्रिया प्रक्रिया आरंभ करना।
- लागू बीसीपी के स्तर पर निर्णय लेना (अर्थात एल1-ए, एल1-बी, एल1-सी)।
- डीएटी में नेटवर्क टीम, डेटा सेंटर टीम, सुविधा टीम, सूचना सुरक्षा टीम, सीआईएसओ आदि के टीम लीडर शामिल होते हैं। क्षति मूल्यांकन समन्वयक, बीसीपी प्रमुख और बीसीपी समन्वयक को क्षति मूल्यांकन प्रगति के बारे में सूचित करेगा और किसी भी मुद्दे की रिपोर्ट करेगा।
- क्षति आकलन के दौरान डीएटी बीसीपी समन्वयक के साथ मिलकर काम करेगा।

- मूल्यांकन पूरा होने के बाद, डीएटी समन्वयक बीसीपी समन्वयक को परिणाम प्रसारित करने के लिए सूचित करेगा। उपलब्ध जानकारी के आधार पर, बीसीपी प्रमुख, बीसीपी समन्वयक और क्षति मूल्यांकन समन्वयक आकस्मिक घटना के स्तर (अर्थात् L1 - a, L1 - b, L1 - c) का निर्धारण करेंगे। आकस्मिक घटना के स्तर के आधार पर यह निर्धारित किया जाएगा कि स्थानांतरण आवश्यक है या नहीं। क्षति मूल्यांकन परिणामों के आधार पर, संचार समन्वयक नागरिक आपातकालीन कर्मियों (जैसे, अग्निशमन, पुलिस) और संबंधित शेयरधारकों को, आवश्यकतानुसार, सूचित करेगा।

22. आपातकाल प्रतिक्रिया टीम की भूमिकाएँ और जिम्मेदारियों

221 मुख्य आपातकाल समन्वयक

मुख्य आपातकालीन समन्वयक विभाग के लिए किसी भी आपातकालीन स्थिति में प्रतिक्रिया की देखरेख करता है। आपातकालीन स्थिति में, इस पद के कर्तव्यों में शामिल हैं:

- निकासी के दौरान, सुनिश्चित करें कि यदि आवश्यक हो तो उचित सहायता बुलाई गई है।
- सुनिश्चित करें कि आपातकालीन प्रतिक्रिया किट कर्मचारी रोस्टर सहित एक नामित स्टाफ सदस्य द्वारा सभा क्षेत्र में लाया जाए।
- सुनिश्चित करें कि आपातकालीन प्रतिक्रिया कर्मचारी निकासी प्रक्रिया शुरू करें तथा निवासियों को निर्देश प्रदान करें।
- निकासी सभा क्षेत्र में, आपातकालीन प्रतिक्रिया कर्मचारियों से स्थिति रिपोर्ट प्राप्त करें। सुनिश्चित करें कि प्रतिक्रिया कर्मचारी आपातकालीन किट में दर्ज रोस्टर का उपयोग करके, कर्मचारियों की संख्या का आकलन करें।
- आने वाले आपातकालीन सेवा कर्मियों से मिलें, उन्हें आपातकालीन स्थिति के स्थान, भवन की रूपरेखा, सहायता की आवश्यकता वाली किसी भी समस्या और कर्मियों के स्थान के बारे में जानकारी प्रदान करें।
- यह सुनिश्चित करने में मदद करें कि भवन में रहने वाले लोग तब तक भवन में प्रवेश न करें जब तक आपातकालीन सेवाओं द्वारा ऐसा करने की अनुमति न दी जाए।
- यदि भवन में ऐसे व्यक्ति हैं जिन्हें विकलांगता के कारण निकासी में सहायता की आवश्यकता है, तो सुनिश्चित करें कि सहायता प्रदान की जाए।
- निरंतर आधार पर यह सुनिश्चित करें कि यह आपातकालीन योजना वर्तमान में जारी रहे।

222 आपातकाल प्रतिक्रिया स्टाफ

- प्रत्येक प्रतिक्रिया स्टाफ सदस्य को भवन के एक निर्दिष्ट क्षेत्र की ज़िम्मेदारी सौंपी गई है। उनका कार्य किसी आपात स्थिति में प्रतिक्रिया के समन्वय में सहायता करना, यह सुनिश्चित करना है कि उचित प्रारंभिक कार्रवाई की गई है, जिसमें यदि आवश्यक हो तो अलार्म सिस्टम को सक्रिय करना और आपातकालीन सहायता बुलाना शामिल है।
- आपातकालीन निकासी के दौरान विशिष्ट जिम्मेदारियों में शामिल हैं:
- अपने क्षेत्र की तुरंत जाँच करें ताकि यह सुनिश्चित हो सके कि सभी को इमारत खाली करने की आवश्यकता के बारे में सूचित कर दिया गया है। इमारत में रहने वाले सभी लोगों को सख्त चेतावनी दें कि वे तुरंत इमारत छोड़ दें। यह जल्दी और ऐसे तरीके से किया जाना चाहिए जिससे आपकी सुरक्षा को कोई खतरा न हो।
- इमारत में रहने वाले सभी लोगों को निर्देश दें कि वे लिफ्ट का इस्तेमाल न करें, बल्कि नज़दीकी सीढ़ी से जाएँ। उन्हें इमारत से बाहर निकलने और पास की इमारत में सबसे नज़दीकी पार्किंग स्थल पर जाने का निर्देश दें।
- यदि निकटतम सीढ़ी धुएं, आग या अन्य खतरों के कारण अवरुद्ध हो, तो वहां रहने वालों को वैकल्पिक निकास की ओर निर्देशित करें।
- यदि किसी व्यक्ति को विकलांगता के कारण सीढ़ियों से नीचे उतरने में सहायता की आवश्यकता हो, तो सुनिश्चित करें कि उसे उचित सहायता प्रदान की जाए।
- निकासी सभा क्षेत्र की ओर बढ़ें और अपने क्षेत्र के कार्मिकों की संख्या का आकलन करें।

- किसी भी समस्या पर मुख्य आपातकालीन समन्वयक को स्थिति रिपोर्ट प्रदान करें, जिसमें वे व्यक्ति शामिल हों जो लापता हैं और अभी भी इमारत में हो सकते हैं, आपातकालीन सेवाओं द्वारा तत्काल सहायता की आवश्यकता वाली कोई भी समस्या, और कोई भी विकलांग व्यक्ति जिसे निकासी सहायता की आवश्यकता है।
- यह सुनिश्चित करने में मदद करें कि आपातकालीन सेवाओं द्वारा अनुमति दिए जाने तक भवन में रहने वाले लोग पुनः प्रवेश न करें।
- आपातकालीन निर्देशों या सूचनाओं के प्रसार में सहायता करना।
- आपातकालीन सेवाओं के पहुंचने पर उन्हें सूचना प्रदान करने में सहायता करें।

23. आपातकालीन स्थितियों पर प्रतिक्रिया के लिए बीसीपी टीमों के लिए दिशानिर्देश

23.1 अग्नि सुरक्षा दिशा-निर्देश

अग्निशमन विधियाँ और निवारक उपाय प्रशासनिक विभाग द्वारा किए जाएंगे

- श्रेणी A, B, C के अग्निशामक यंत्रों को उचित संख्या में परिसर में सुलभ स्थानों पर और उनका रिकॉर्ड रखना । ज़िम्मेदारी: प्रशासन
- सभी अग्निशामक यंत्रों का हर महीने निरीक्षण किया जाता है और उसका रिकॉर्ड रखा जाता है। ज़िम्मेदारी: प्रशासन प्रशासन
- यह सुनिश्चित किया जाता है कि निम्नलिखित को सभी उपयुक्त स्थानों पर प्रदर्शित किया जाए और इसका रिकॉर्ड रखा जाए
- आपातकालीन निकासी योजनाएँ,
- फ्लोरोसेंट आपातकालीन निकास साइन बोर्ड
- ईआरटी सदस्यों की सूची
- आपातकालीन टेलीफोन/मोबाइल नंबरों की सूची।
- विभिन्न अनुभागों से उचित संख्या में कर्मचारियों वाली एक आपातकालीन प्रतिक्रिया टीम (ERT) बनाई जाती है। यह सुनिश्चित किया जाता है कि ERT के सभी सदस्य, सुरक्षा गार्ड, प्रशासन, मानव संसाधन सभी अग्निशमन में प्रशिक्षित हों। अभिलेखों का रखरखाव किया जाना चाहिए।
- सभी मौजूदा और नए कर्मचारियों को अग्नि सुरक्षा दिशानिर्देशों का प्रशिक्षण दिया जाता है। रिकॉर्ड बनाए रखना अनिवार्य है।
- अग्नि अभ्यास कम से कम अर्धवार्षिक रूप से किया जाना चाहिए, तथा इसका रिकार्ड रखा जाना चाहिए।
- विभिन्न अनुभागों से उचित संख्या में कर्मचारियों को लेकर प्राथमिक चिकित्सा प्रशिक्षित कार्मिक (एफएटीपी) की एक टीम बनाई जाती है।

23.2 आग लगने की स्थिति में

- अलार्म बजाएँ। अलार्म बजने पर तुरंत प्रतिक्रिया दें। जिन इमारतों में फायर अलार्म सिस्टम नहीं है, वहाँ रहने वालों को मौखिक रूप से सूचित करें।
- प्रशासन विभाग या मानव संसाधन विभाग को कॉल करें।
- निम्नलिखित जानकारी प्रदान करें:
  - आपका नाम और स्थान
  - आग लगने का स्थान
  - अनुरोधित विवरण
- जितनी जल्दी हो सके इमारत से बाहर निकलें। घबराएँ नहीं।
- आग से निपटने के लिए तब तक कोई प्रयास नहीं किया जाना चाहिए जब तक कि वह कार्रवाई सभी संबंधितों की सुरक्षा के अनुकूल न हो। प्रशासन/मानव संसाधन/आपातकालीन प्रतिक्रिया दल ('ईआरटी') से आगे के निर्देशों की प्रतीक्षा करें। केवल प्रशासन/मानव संसाधन/ईआरटी के निर्देशों का पालन करें क्योंकि उन्हें ऐसी स्थितियों से निपटने का प्रशिक्षण दिया गया है।
- किसी भी मूल्यवान वस्तु या कार्य-संबंधी सामग्री को बचाने का प्रयास न करें क्योंकि इससे निकासी प्रक्रिया में बाधा उत्पन्न हो सकती है।
- जब तक प्रशासन/एचआर/ईआरटी द्वारा निर्देश न दिया जाए, निकास द्वार को छोड़कर खिड़कियां या बंद दरवाजे न तोड़ें।
- लिफ्ट/एलेवेटर का इस्तेमाल न करें क्योंकि लिफ्ट/एलेवेटर शाफ्ट में मौजूद ऑक्सीजन आग को बढ़ने में मदद करती है। नज़दीकी निकास द्वार का इस्तेमाल करें।

- व्यवस्थित लेकिन तेज़ गति से बाहर निकलें। आपातकालीन निकास की ओर ले जाने वाले स्वतः प्रकाशित होने वाले संकेतों का पालन करें। अगर आप घने धुएँ में फँस जाएँ, तो नाक से छोटी साँसें लें और रेंगते हुए निकटतम आपातकालीन निकास द्वार तक जाएँ, क्योंकि ज़मीन के सबसे पास की हवा में साँस लेना ज़्यादा आसान होगा।
- वृद्धजनों, शारीरिक रूप से अक्षम लोगों की सहायता तभी करें जब आप ऐसा करने की स्थिति में हों।
- कोई भी दरवाज़ा खोलते समय बेहद सावधानी बरतें। गर्मी का एहसास होने पर दरवाज़ा अपने सामने रखें और सुरक्षा के लिए उसे अपने सामने रखें।
- यदि उपलब्ध हो तो धुंआ बाहर रखने के लिए दरवाजे के नीचे एक गीला कपड़ा रखें।
- अगर आप किसी केबिन में फँस गए हैं, तो खिड़की पर "सेव आवर सोल्स" (SOS) का साइन बोर्ड लगा दें ताकि अग्निशमन कर्मी उसे देख सकें। अगर आपके ऑफिस की खिड़कियाँ काली हैं, तो ध्यान आकर्षित करने के लिए टॉर्च का इस्तेमाल करें। आग लगने के खतरे को छोड़कर, कभी भी खिड़की न तोड़ें।

233 आग लगने के बाद

- प्राथमिक चिकित्सा प्रशिक्षित कार्मिक (FATP) आवश्यकतानुसार सहायता प्रदान करते हैं। गंभीर रूप से घायल या जले हुए पीड़ितों को तुरंत प्रोफेशनल चिकित्सा सहायता प्रदान की जानी चाहिए।
- क्षतिग्रस्त परिसर से दूर रहें। केवल तभी लौटें जब प्रशासन/मानव संसाधन/ईआरटी सूचित करें कि यह सुरक्षित है।

234 मानव संसाधन जिम्मेदारियां

- आग लगने के दौरान असेंबली का प्रबंधन करें
- सुनिश्चित करें कि सभी प्रवेशित कर्मचारी बाहर निकल गए हैं

235 फायर ड्रिल

- फायर ड्रिल हर तिमाही आयोजित की जाती है और प्रशासन इसका रिकॉर्ड रखता है।
- मानव संसाधन विभाग फायर ड्रिल के दिन उपस्थित कर्मचारियों की सूची तैयार करता है ताकि रोल कॉल सही ढंग से लिया जा सके। विचलन रिपोर्ट तैयार की जाती है और प्रशासन/प्रबंधन को सूचित की जाती है।
- एचआर असेंबली के प्रबंधन में मदद के लिए डिस्प्ले में प्रदर्शित करता है।
- प्रशासन प्रभावी निकासी/अग्नि अभ्यास के समय का ध्यान रखें।
- फायर ड्रिल प्रभावशीलता रिपोर्ट आईटी विभाग को भेजी जाती है।
- रिपोर्ट में निम्नलिखित शामिल हैं:
  - जनशक्ति की सूची में विचलन
  - प्रभावी फायर ड्रिल समय
  - अनुशासन
  - अन्य जानकारी, अगर कोई हो तो ।

236 भूकंप

निम्नलिखित प्रक्रियाएं उन बड़े भूकंपों पर लागू होती हैं जो तीव्र कंपन पैदा करते हैं:

- अगर घर के अंदर हैं, तो नीचे गिरें, ढकें और पकड़ें। खुद को गिरती हुई वस्तुओं जैसे लाइट फिक्स्चर, किताबों की अलमारी, कैबिनेट, शेल्फ और अन्य फर्नीचर से बचाएँ जो फिसलकर गिर सकते हैं। खिड़कियों से दूर रहें। हो सके तो किसी मेज़ या डेस्क के नीचे छिप जाएँ। उसे थामे रहें और उसके साथ चलने के लिए तैयार रहें। अगर कोई आश्रय उपलब्ध न हो, तो किसी अंदरूनी दीवार से ढँक लें और अपने सिर और गर्दन को अपनी बाँहों से सुरक्षित रखें।
- दरवाज़े के पास खड़े न हों। दरवाज़े के पास जाने की भूकंप सुरक्षा प्रक्रिया पुरानी हो चुकी है, और दरवाज़े किसी भी अन्य जगह से ज़्यादा सुरक्षा प्रदान नहीं करते। दरअसल, भूकंप के दौरान दरवाज़े की ओर बढ़ते या वहाँ खड़े होते समय कुछ लोग घायल भी हुए हैं।
- अगर आप बाहर हैं, तो इमारतों, बिजली के खंभों या अन्य संभावित खतरों से दूर रहें। खुले क्षेत्र में रहें।

- भूकंप के दौरान, बाहर निकलने के लिए न भागें या इमारत से बाहर निकलने का प्रयास न करें, क्योंकि आपके रास्ते में भारी वस्तुएं या मलबा गिर सकता है।
- लिफ्ट का प्रयोग न करें।
- जब कंपन रुक जाए, तो अपने आस-पास के लोगों को लगी चोटों की जाँच करें। गंभीर रूप से घायल लोगों को तब तक हिलाने की कोशिश न करें जब तक कि उन्हें तत्काल खतरा न हो। ज़रूरत पड़ने पर प्राथमिक उपचार प्रदान करें।
- इमारत को नुकसान, आग, ज्वलनशील या दहनशील तरल पदार्थों का रिसाव, या ज्वलनशील गैसों का रिसाव जैसे सुरक्षा खतरों के लिए क्षेत्र की जाँच करें। यदि क्षेत्र या इमारत असुरक्षित प्रतीत होती है, तो निकासी प्रक्रिया शुरू करें।
- यदि ऐसा करना सुरक्षित हो तो घर खाली करने से पहले बिजली के उपकरण और गैस के स्रोत बंद कर दें।
- इमारत से बाहर निकलें और चोटों, क्षति और संभावित खतरनाक स्थितियों की रिपोर्ट करने के लिए सभा स्थल पर जाएं।
- किसी भी गंभीर चोट या अन्य तत्काल आपात स्थिति की सूचना देने के लिए एम्बुलेंस को कॉल करें।
- एक बार जब आप भवन से बाहर निकल जाएं, तो तब तक दोबारा प्रवेश न करें जब तक कि प्रशिक्षित आपातकालीन कर्मियों द्वारा भवन का निरीक्षण न कर लिया जाए।

237 बिजली कटौती

बिजली कटौती की प्रतिक्रिया परिस्थितियों पर निर्भर करेगी। यदि संभव हो, तो सुविधा टीम से कटौती की सीमा और संभावित अवधि के बारे में जानकारी प्राप्त की जानी चाहिए।

- क्षति मूल्यांकन टीम आपके क्षेत्र में कटौती की सीमा का आकलन करेगी और मुख्य आपातकालीन समन्वयक और बीसीपी समन्वयक को स्थिति की रिपोर्ट देगी।
- अंधेरे क्षेत्रों में फंसे लोगों को सुरक्षित स्थान पर जाने में सहायता करें।
- लिफ्ट की जाँच करें और पता लगाएँ कि अंदर कोई फँसा तो नहीं है। अगर ऐसा है, तो तुरंत मदद के लिए पुकारें; दरवाज़ा ज़बरदस्ती खोलकर उन्हें बचाने की कोशिश न करें। किसी योग्य लिफ्ट मैकेनिक का इंतज़ार करें।
- बिजली कटौती के दौरान डेस्कटॉप कंप्यूटर, उपकरण और उपकरणों को अनप्लग कर दें, विशेषकर यदि वे सर्ज प्रोटेक्टर से कनेक्ट नहीं हैं।
- किसी भी उपकरण या प्रक्रिया को बंद कर दें जो बिजली अचानक वापस आने पर खतरनाक हो सकती है।
- मुख्य आपातकालीन समन्वयक से यह निर्देश मांगें कि स्थान खाली करना है या वहीं रहना है।

238 आपातकाल चिकित्सा

आपातकाल की स्थिति में चिकित्सा:

सहायता के लिए 102 पर कॉल करें। निम्नलिखित जानकारी प्रदान करें:

- इमारत का पता और फ़ोन नंबर
- मंज़िल या कमरा नंबर
- चोट की प्रकृति
- घायल व्यक्ति का स्थान
- घायल व्यक्ति की आयु
- घायल व्यक्ति का लिंग
- वर्तमान स्थिति

- कोई ज्ञात चिकित्सा इतिहास

इसके अलावा, मुख्य आपातकालीन समन्वयक और आपातकालीन प्रतिक्रिया स्टाफ को सूचित करें।
चिकित्सा संबंधी आपात स्थिति वाले व्यक्ति के साथ रहें। जब तक उन्हें और अधिक चोट लगने का तत्काल खतरा न हो, उन्हें न हिलाएँ।

23.9 बम खतरा प्रक्रियाएँ

- हडको कार्मिकों को टेलीफोन पर बम की धमकी मिलने पर नीचे दिए गए फॉर्म का उपयोग करते हुए, कॉल करने वाले से यथासंभव अधिक जानकारी प्राप्त करनी चाहिए, तथा इसकी सूचना तुरंत पुलिस विभाग (100) को देनी चाहिए।
- डाक या अन्य माध्यम से प्राप्त बम की धमकी की सूचना भी तुरंत पुलिस विभाग (100) को दी जानी चाहिए।
- बम निरोधक दस्ता खतरे का आकलन करेगा और यदि आवश्यक हो तो भवन खाली करने की सलाह भवन में रहने वालों को देगा।
- यदि खाली करना आवश्यक हो, तो मुख्य आपातकालीन समन्वयक आपातकालीन प्रतिक्रिया कर्मचारियों के साथ मिलकर भवन में रहने वाले सभी लोगों को पार्किंग स्थल में एकत्रित करेंगे तथा वापस लौटने की सलाह मिलने तक भवन से 300 फीट की दूरी पर रहेंगे।

23.10 विकलांग व्यक्तियों के लिए आपातकाल निकास

अधिक से अधिक जानकारी एकत्र करने के लिए कॉल करने वाले से पूछे जाने वाले प्रश्न:

1. बम कब विस्फोट होगा?
2. बम अभी कहाँ है ?
3. यह कैसा दिखता है?
4. यह किस प्रकार का बम है?
5. यह किस कारण से फटेगा?
6. क्या आपने बम रखा है?
7. क्यों?
8. आपका पता क्या है?
9. आपका नाम क्या है?

यह खंड आग और अन्य भवन आपात स्थितियों के दौरान विकलांग व्यक्तियों के लिए निकासी प्रक्रियाओं के सामान्य दिशानिर्देश प्रदान करता है। विकलांग व्यक्तियों को अपने प्राथमिक और द्वितीयक निकासी मार्गों की पहचान करनी चाहिए, और ऐसे सहयोगियों की तलाश करनी चाहिए जो निकासी सहायक के रूप में सेवा करने के इच्छुक हों। अन्य कर्मचारी उन लोगों के बारे में जागरूक होकर मदद कर सकते हैं जिन्हें निकासी में सहायता की आवश्यकता हो सकती है।

गतिशीलता-बाधित -व्हीलचेयर

ज़्यादातर इमारतों में लोगों को इमारत से बाहर निकलने के लिए सीढ़ियों का इस्तेमाल करना पड़ता है। लिफ्ट का इस्तेमाल नहीं किया जा सकता क्योंकि आपात स्थिति में इन्हें असुरक्षित माना गया है।

पहली मंजिल पर व्हीलचेयर पर बैठे लोग, बाहरी भूतल पर जाने के लिए इमारत के निकास द्वार का उपयोग कर सकते हैं। ऊपरी मंजिलों पर रहने वाले विकलांग व्यक्तियों के लिए, व्हीलचेयर को सीढ़ियों से नीचे ले जाने का प्रयास करना सुरक्षित नहीं है।

स्थिति से निपटने का एक प्रभावी तरीका निम्नलिखित है:

स्थान पर ठहरो

एक निकासी सहायक के साथ काम करते हुए, एक ऐसा कमरा चुनें जिसमें बाहरी खिड़की, टेलीफ़ोन और एक मज़बूत या आग प्रतिरोधी दरवाज़ा हो। इस कमरे में विकलांग व्यक्ति के साथ रहें, और किसी व्यक्ति को निकासी क्षेत्र में भेजकर आपातकालीन कर्मियों को सहायता की आवश्यकता वाले व्यक्ति के स्थान की सूचना दें। विकलांग व्यक्ति को सहायता की प्रतीक्षा में सीढ़ियों के पास भी रखा जा सकता है, हालाँकि यह क्षेत्र धुएँ और अन्य खतरों से सुरक्षित नहीं हो सकता है।

आपातकालीन बचाव में प्रशिक्षित अग्निशमन विभाग के कर्मचारी, इमारत में प्रवेश कर सकते हैं और व्यक्ति को इमारत से बाहर निकलने में सहायता कर सकते हैं, या तो सीढ़ियों से नीचे उतरकर या आपातकालीन लिफ्ट का उपयोग करके।

अपने स्थान पर रहते हुए, व्हीलचेयर उपयोगकर्ता को आपातकालीन सेवाओं के संपर्क में रहना चाहिए तथा अपने स्थान की सीधे सूचना देनी चाहिए।

व्हीलचेयर उपयोगकर्ताओं को सीढ़ियों से बाहर निकालने का काम अग्निशमन विभाग के प्रशिक्षित प्रोफेशनलों द्वारा किया जाना चाहिए। केवल अत्यधिक खतरे की स्थिति में ही अप्रशिक्षित लोगों को व्हीलचेयर उपयोगकर्ताओं को बाहर निकालने का प्रयास करना चाहिए। यदि ऐसा करना आवश्यक हो, तो एक विकल्प निम्नलिखित है:

व्यक्ति पालना ढोना

- तब तक प्रतीक्षा करें जब तक कि अन्य लोग सीढ़ियों से नीचे न उतर जाएँ।
- दो सहायक व्यक्ति के दोनों ओर खड़े होते हैं।
- वे व्यक्ति के पास पहुँचते हैं और उसे पालने में उठाकर बाहर निकालते हैं।
- सहायक धीरे-धीरे और सावधानी से चलकर नीचे उतरने को नियंत्रित करते हैं।

व्हीलचेयर को कभी भी सीढ़ियों पर न छोड़ें।

- कार्यालय की कुर्सी से निकासी.
- शारीरिक रूप से विकलांग व्यक्ति को एक मजबूत कार्यालय कुर्सी पर स्थानांतरित करें
- एक सहायक कुर्सी को धीरे से पीछे की ओर झुकाता है।
- दूसरा सहायक कुर्सी की ओर मुँह करके कुर्सी के अगले पैरों को पकड़ेगा। दोनों एक साथ कुर्सी उठाएँगे।
- सहायक अपने पैरों को धीरे-धीरे मोड़कर और अपनी पीठ को सीधा रखकर उतराई को नियंत्रित करते हैं।

गतिशीलता बाधित - गैर-व्हीलचेयर

गतिशीलता में अक्षम व्यक्ति जो स्वतंत्र रूप से चलने में सक्षम हैं, उन्हें आपात स्थिति में थोड़ी सी सहायता से सीढ़ियाँ चढ़ने में सक्षम होना चाहिए। व्यक्ति को बाहर निकलने का प्रयास करने से पहले सीढ़ियों पर भारी यातायात के हटने तक प्रतीक्षा करनी चाहिए।

श्रवण बाधित

श्रवण बाधित व्यक्ति ऑडियो आपातकालीन अलार्म नहीं सुन सकते हैं, तथा उन्हें आपातकालीन स्थितियों के बारे में भवन में रहने वाले अन्य लोगों द्वारा सचेत किए जाने की आवश्यकता होगी।

दृष्टिबाधित

अधिकांश दृष्टिबाधित व्यक्ति अपने आस-पास के वातावरण और अक्सर यात्रा किए जाने वाले मार्गों से परिचित होंगे। चूँकि आपातकालीन निकासी मार्ग सामान्यतः यात्रा किए जाने वाले मार्ग से भिन्न हो सकता है, इसलिए दृष्टिबाधित व्यक्तियों को निकासी में सहायता की आवश्यकता हो सकती है। सहायक को दृष्टिबाधित व्यक्ति को अपनी कोहनी दिखानी चाहिए और उसे निकासी मार्ग पर मार्गदर्शन करना चाहिए। निकासी के दौरान, सहायक को सुरक्षित निकासी सुनिश्चित करने के लिए आवश्यकतानुसार संवाद करना चाहिए। आपातकालीन प्रतिक्रिया कर्मचारियों को किसी भी आपात स्थिति से पहले अपने क्षेत्र में विशेष आवश्यकताओं वाले भवन निवासियों की आवश्यकताओं का आकलन करना चाहिए। पूछें कि क्या कोई कर्मचारी है जिसे निकासी की स्थिति में सहायता की आवश्यकता होगी, और आस-पास के व्यक्तियों को निकासी सहायक के रूप में सेवा देने की व्यवस्था करें।

24. घटना रिपोर्टिंग संपर्क

हडको को घटना रिपोर्टिंग संपर्क सूची बनाए रखनी होगी।

क्रम सं..	पद नाम	सेवा/विभाग	संपर्क नं.	जगह

25. आपातकाल सेवाएँ

न्यूनतम कर्मचारी मांग: के लिए सूची का न्यूनतम कर्मचारी आवश्यक द्वारा विभिन्न न्यूनतम कर्मचारी आवश्यकता: विभिन्न विभागों द्वारा अपेक्षित न्यूनतम कर्मचारियों की सूची

क्र.सं.	आपातकाल संपर्क	आपातकाल नहीं
1	दिल्ली पुलिस विभाग	100/112
2	दिल्ली आग विभाग	101
3	एम्बुलेंस	108
4	केंद्रीय दुर्घटना और आघात सेवाएँ	102/1099
6	आपदा प्रबंधन एवं शमन इकाई, नेहरू प्लेस, नई दिल्ली	+91- 7947106659

एक बार बीसीपी शुरू हो जाने के बाद, प्रत्येक बीसीपी इकाई समन्वयक को यह सुनिश्चित करना होगा कि न्यूनतम कर्मचारी आवश्यकता पूरी हो, इसके लिए उन्हें या तो भौतिक रूप से वर्कस्टेशन प्रदान करना होगा या संचालन आवश्यकता को पूरा करने के लिए इंटरनेट डोंगल प्रदान करना होगा।

- प्रक्रिया निर्भरता रिकॉर्ड: सुचारू संचालन कार्य के लिए, बीसीपी इकाई समन्वयक को यह सुनिश्चित करना होगा कि प्रक्रियाओं की अपस्ट्रीम और डाउनस्ट्रीम दोनों निर्भरताएं काम कर रही हैं।
- आरटीओ और आरपीओ: आईटी समन्वयक को यह सुनिश्चित करना होगा कि उनकी रिकवरी प्रणालियां इन समयसीमाओं का पालन करें।

- संसाधन/आपूर्ति आवश्यकता: प्रत्येक प्रशासन/अवसंरचना समन्वयक को यह सुनिश्चित करना होगा कि किसी भी आकस्मिकता के लिए प्रत्येक साइट पर न्यूनतम संसाधन/आपूर्ति आवश्यकता उपलब्ध हो।
- गंभीर अवधि: गंभीर अवधि व्यावसायिक घंटे की त्वरितता पर्यटन को प्रभावित करती है।
- आपातकालीन स्थिति में, प्रशासन व्यवस्थापक समन्वयक या किसी अन्य बीसीपी संगठन के सदस्य को विक्रेता सेवाओं को बहाल करने के लिए इस सूची का उपयोग करना होगा।

26. अभ्यास और सत्यापन अवधारणा

26.1 अभ्यास के उद्देश्य

पुनर्प्राप्ति प्रक्रिया का संपूर्ण और कठोर परीक्षण करना, जिसमें विघटनकारी घटना का अनुकरण भी शामिल है, जिससे ऐसे परिणाम प्राप्त होते हैं जिन्हें मापा और मूल्यांकन किया जा सकता है, साथ ही फीडबैक भी प्राप्त होता है जो बीसीपी को बेहतर और सुव्यवस्थित बनाने में सक्षम बनाता है।

26.2 अभ्यास दायरा

ये परीक्षण व्यापक और विस्तृत तरीके से किए जाएँगे ताकि योजना के सभी पहलुओं का परीक्षण किया जा सके। इन परीक्षणों में संगठन की सभी व्यावसायिक और सहायक इकाइयाँ योगदान देंगी।

26.3 अभ्यास अनसूची

बीसीपी समन्वयक द्वारा बीसीपी टीम और व्यवसाय प्रबंधन टीमों के साथ मिलकर नियमित आधार पर एक व्यवसाय निरंतरता योजना अभ्यास/परीक्षण निर्धारित किया जाएगा। अभ्यासों को मौसमी उत्पादन और व्यावसायिक चक्र जैसे कारकों को ध्यान में रखते हुए निर्धारित किया जाएगा।

26.4 अभ्यास पद्यति

व्यवसाय निरंतरता योजनाओं और व्यवसाय प्रक्रिया तथा नैदानिक क्षेत्रों के लिए परिभाषित वैकल्पिक प्रसंस्करण कौशलनीतियों दोनों को मान्य करने के लिए परीक्षणों और अभ्यासों का एक संयोजन आयोजित किया जाएगा। आवश्यकतानुसार सभी अभ्यास विधियों का क्रियान्वयन किया जाएगा।

26.5 घोषित और अघोषित अभ्यास

घोषित अभ्यास निर्धारित अभ्यास होते हैं, जैसे कि वैकल्पिक सुविधा पर कंप्यूटर प्रोसेसिंग की वास्तविक बहाली से जुड़े अभ्यास, जिसके दौरान आमतौर पर उत्पादन प्रक्रिया बाधित नहीं होती, लेकिन वास्तविक बहाली और सत्यापन के लिए योजना बनाई जा सकती है। इस प्रकार के परीक्षण में संपूर्ण व्यावसायिक निरंतरता संगठन शामिल नहीं होगा, बल्कि इसमें कंप्यूटर संचालन और तकनीकी कर्मचारियों के साथ-साथ चुनिंदा उपयोगकर्ता (पुनर्प्राप्त किए जा रहे अनुप्रयोगों से जुड़े) शामिल होंगे।

अघोषित अभ्यास अचानक किए जाने वाले अभ्यास होते हैं जिनमें व्यवसाय निरंतरता संगठन का केवल एक छोटा सा हिस्सा और कुछ ही उपयोगकर्ता, यदि कोई हों, शामिल होंगे। कॉल सूचना और टेबलटॉप ऐसे अभ्यास हैं जिन्हें अघोषित किया जा सकता है क्योंकि इनका वास्तविक व्यावसायिक कार्यों पर सबसे कम प्रभाव/बाधा होगी। अघोषित अभ्यास व्यवसाय इकाई प्रबंधन के विवेक पर किए जाएँगे।

26.6 मूल्यांकन का अभ्यास

सभी अभ्यासों के परिणामों का मूल्यांकन एक निष्पक्ष सत्यापन टीम द्वारा किया जाएगा। यह टीम हडको से बनी होगी और इसका पूरा ध्यान व्यावसायिक व्यवधान/आपदा की स्थिति में हडको की महत्वपूर्ण व्यावसायिक प्रक्रियाओं को फिर से शुरू करने की योजना की निरंतर वैधता, प्रासंगिकता और क्षमता का मूल्यांकन करने पर केंद्रित होगा। अभ्यास सत्यापन टीम के पास निम्नलिखित जिम्मेदारियां होती हैं:

- अभ्यास के दायरे में समग्र व्यवसाय निरंतरता योजना(ओं) से परिचित होना।
- आयोजित किए जाने वाले अभ्यास के उद्देश्यों को अच्छी तरह से समझना।

- अभ्यास में शामिल प्रबंधन टीमों और कर्मचारियों की सभी गतिविधियों की निगरानी और अवलोकन करना।
- यह सुनिश्चित करना कि आईटी और अन्य शेयरधारकों के दृष्टिकोण से अभ्यास के उद्देश्य पूरे हों।
- अभ्यास के दौरान देखी गई शक्तियों और कमजोरियों से संबंधित निष्कर्षों का दस्तावेजीकरण करना।
- व्यवसाय प्रक्रिया/योजना ओनर के साथ अनुवर्ती कार्रवाई करके यह पता लगाना कि क्या आवश्यक परिवर्तन पूरे कर लिए गए हैं।
- अभ्यास सत्यापन टीम की कार्रवाइयों के अतिरिक्त, व्यवसाय प्रक्रिया प्रबंधन/कर्मचारियों के प्रत्येक प्रतिभागी से अभ्यास की प्रभावशीलता, सफलता और मूल्य का मूल्यांकन करने के लिए कहा जाएगा।

267 अभ्यास के बाद रिपोर्टिंग

अभ्यास प्रक्रिया प्रबंधन/कर्मचारी, परीक्षण/अभ्यास समन्वयक के साथ मिलकर, यथाशीघ्र, लेकिन घोषित या अघोषित अभ्यास के पूरा होने के तीन सप्ताह के बाद, अभ्यास के परिणामों का दस्तावेजीकरण करेंगे।

व्यावसायिक इकाई प्रबंधन टीम के चयनित सदस्य अभ्यास के परिणामों की समीक्षा करेंगे और पहचानी गई किसी भी कमी को दूर करने के लिए आवश्यक कार्रवाई की पहचान करेंगे। बीसीपी समन्वयक समीक्षा का प्रबंधन करेगा और योजना में उचित परिवर्तन/अद्यतन का समन्वय करेगा। समीक्षा के परिणाम प्रबंधन टीम के समक्ष प्रस्तुत किए जाएँगे।

268 परिवर्तन प्रबंधन प्रक्रिया (सीखे गए सबक के जवाब में)

बीसीपी में आवश्यक किसी भी बदलाव को शामिल करने के लिए औपचारिक परिवर्तन प्रबंधन लागू किया जाता है। बीसीपी में निहित जटिलता के स्तर के कारण यह आवश्यक है।

27. प्रशिक्षण और जागरूकता

प्रशिक्षण और जागरूकता कार्यक्रम सहयोगियों को पुनर्प्राप्ति प्रक्रिया में उनकी भूमिकाओं के लिए तैयार करते हैं और बीसीएम योजनाओं को विकसित करने, लागू करने, बनाए रखने और क्रियान्वित करने के लिए आवश्यक कौशल को निरंतर बढ़ाते हैं। ये कार्यक्रम तत्परता की एक ऐसी स्थिति भी बनाते हैं जो सहयोगियों और व्यवसाय की सुरक्षा सुनिश्चित करने में मदद करेगी।

व्यवहार्य निरंतरता क्षमता की आवश्यकता और उसे बनाए रखने की प्रक्रिया के बारे में जागरूकता आवश्यक है। हडको में हम इसे औपचारिक शिक्षा और प्रशिक्षण सत्रों के माध्यम से प्राप्त करेंगे, जो आवश्यकतानुसार आयोजित किए जाएँगे। यह व्यवसाय निरंतरता कार्यक्रम और प्रक्रियाओं के बारे में आवश्यक जागरूकता और समझ प्रदान करने का एक तरीका है ताकि स्थानीय व्यवसाय निरंतरता योजनाओं के साथ-साथ समग्र व्यवसाय निरंतरता उद्देश्यों को उन कर्मियों द्वारा समझा जा सके जो निरंतरता/पुनर्प्राप्ति प्रक्रियाओं को बनाए रखने और क्रियान्वित करने के लिए ज़िम्मेदार हैं।

हडको को सभी स्तरों पर कर्मचारियों के लिए विभिन्न अनिवार्य और गैर-अनिवार्य प्रशिक्षणों को परिभाषित करना चाहिए।

उद्देश्य

- उन प्रमुख कर्मचारियों और प्रबंधन कार्मिकों को प्रशिक्षित करें जिन्हें योजना को निरंतर तत्परता की स्थिति में बनाए रखने की आवश्यकता है।
- प्रमुख कर्मचारियों और प्रबंधन कार्मिकों को उनकी भूमिकाओं और जिम्मेदारियों में प्रशिक्षित करना, जिन्हें सभी/विभिन्न योजना खंडों को निष्पादित करने और व्यवधान/आउटेज या विनाशकारी आपदा की स्थिति में महत्वपूर्ण व्यावसायिक प्रसंस्करण को बनाए रखने के लिए वैकल्पिक प्रसंस्करण कौशलनीतियों को लागू करने की आवश्यकता होती है।

- संचार प्रक्रिया पर प्रमुख कर्मचारियों और प्रबंधन कर्मियों को प्रशिक्षित करें और उन लोगों के लिए जिम्मेदारियां जो व्यवसाय व्यवधान/आउटेज से प्रभावित होंगे और महत्वपूर्ण प्रसंस्करण में रुकावट के दौरान क्या अपेक्षित है।
- योजना के रखरखाव और/या क्रियान्वयन में सीधे तौर पर शामिल न होने वाले कर्मचारियों के लिए योजना जागरूकता को बढ़ाना।

28. रखरखाव प्रोटोकॉल की योजना

बोर्ड हडको की व्यवसाय निरंतरता योजना को अनुमोदित करने के लिए ज़िम्मेदार है। कार्यकारी निदेशक (आईटी) को योजना को क्रियान्वित करने और उसकी आवश्यक वार्षिक समीक्षा करने का अधिकार है। निम्नलिखित स्थितियों के उत्पन्न होने पर बीसीपी में बार-बार संशोधन किया जाएगा:

- प्रमुख तकनीकी परिवर्तन होते हैं
- ग्राहक सूचना की संवेदनशीलता बढ़ जाती है।
- सूचना परिवर्तन के लिए आंतरिक या बाह्य खतरे।

जब भी हडको के संचालन, संरचना, व्यवसाय या स्थान, या हडको के साझेदारों के संचालन में कोई महत्वपूर्ण परिवर्तन होगा, हडको इस योजना को अद्यतन करेगा। इसके अतिरिक्त, हडको इस व्यवसाय निरंतरता योजना की वार्षिक समीक्षा करेगा और संचालन, संरचना, व्यवसाय या स्थान में होने वाले परिवर्तनों के अनुसार इसे संशोधित करेगा।

हडको अपनी बीसीपी की प्रतियाँ निरीक्षण के लिए, वार्षिक समीक्षा और योजना में किए गए परिवर्तनों के साथ रखता है। योजना की एक इलेक्ट्रॉनिक प्रति हडको के स्थानीय और ऑनलाइन दस्तावेज़ संग्रह में उपलब्ध है।

28.1 टीमें और जिम्मेदारियाँ

बीसीपी प्रमुख बीसीपी के समग्र नियंत्रण में रहेंगे, लेकिन अन्य समन्वयक बीसीपी के अपने-अपने अनुभागों में आवश्यक परिवर्तनों पर अपनी राय देंगे। यह महत्वपूर्ण है कि संबंधित बीसीपी समन्वयकों को योजना में किसी भी स्वीकृत परिवर्तन के बारे में पूरी जानकारी दी जाए।

28.2 योजना को अद्यतन करने के लिए परिवर्तन नियंत्रण प्रक्रिया

बीसीपी में निहित जटिलता के स्तर के कारण यह आवश्यक है कि बीसीपी में आवश्यक किसी भी बदलाव को शामिल करने के लिए औपचारिक परिवर्तन प्रबंधन लागू किया जाता है।

28.3 रखरखाव अनुसूची

अनुसूचित रखरखाव में अर्ध-वार्षिक संरचित पूर्वाभ्यास और/या सामरिक अभ्यासों के परिणामों पर आधारित अद्यतन आवश्यकताएँ शामिल होती हैं। अर्ध-वार्षिक योजना समीक्षा का उद्देश्य यह निर्धारित करना है कि क्या व्यवसाय निरंतरता योजना(ओं) से संबंधित कौशलनीतियों, कार्यों/प्रक्रियाओं, संसाधन आवश्यकताओं, टीम असाइनमेंट, अधिसूचना और प्रशासनिक मुद्दों में परिवर्तन आवश्यक हैं।

बीसीपी समन्वयक अनुसूचित रखरखाव गतिविधियों को आरंभ करने और समन्वय करने के लिए जिम्मेदार होता है।

29. घटना प्रतिक्रिया योजना

29.1 साइबर घटना प्रतिक्रिया के लक्ष्य

जब कोई साइबर सुरक्षा घटना घटती है, तो घटना के प्रभाव को प्रबंधित करने के लिए समय पर और पूरी तरह से कार्रवाई करना एक प्रभावी प्रतिक्रिया प्रक्रिया के लिए महत्वपूर्ण है। प्रतिक्रिया को यह सुनिश्चित करके संभावित नुकसान को सीमित करना चाहिए कि कार्रवाई सुविचारित और समन्वित हो। विशेष रूप से, प्रतिक्रिया के लक्ष्य ये हैं:

1. घटक और कर्मचारी सूचना की गोपनीयता को संरक्षित और सुरक्षित रखना तथा प्रणालियों, नेटवर्क और संबंधित डेटा की अखंडता और उपलब्धता सुनिश्चित करना।
2. कंप्यूटर या नेटवर्क सुरक्षा घटना या अन्य प्रकार के डेटा उल्लंघन के बाद व्यावसायिक प्रक्रियाओं को पुनर्प्राप्त करने में सहायता करें।
3. सिस्टम और नेटवर्क खतरों के लिए एक सुसंगत प्रतिक्रिया कौशलनीति प्रदान करें जो डेटा और सिस्टम को जोखिम में डालते हैं।
4. घटना की प्रारंभिक रिपोर्टिंग के साथ-साथ आवश्यकतानुसार निरंतर संचार सहित एक संचार योजना विकसित और सक्रिय करें।
5. बाह्य कंप्यूटर घटना प्रतिक्रिया टीमों और कानून प्रवर्तन के साथ प्रयासों का समन्वय करना।
6. संगठनों की प्रतिष्ठा संबंधी जोखिम को न्यूनतम करें।

29.2 उद्देश्य और स्कोप

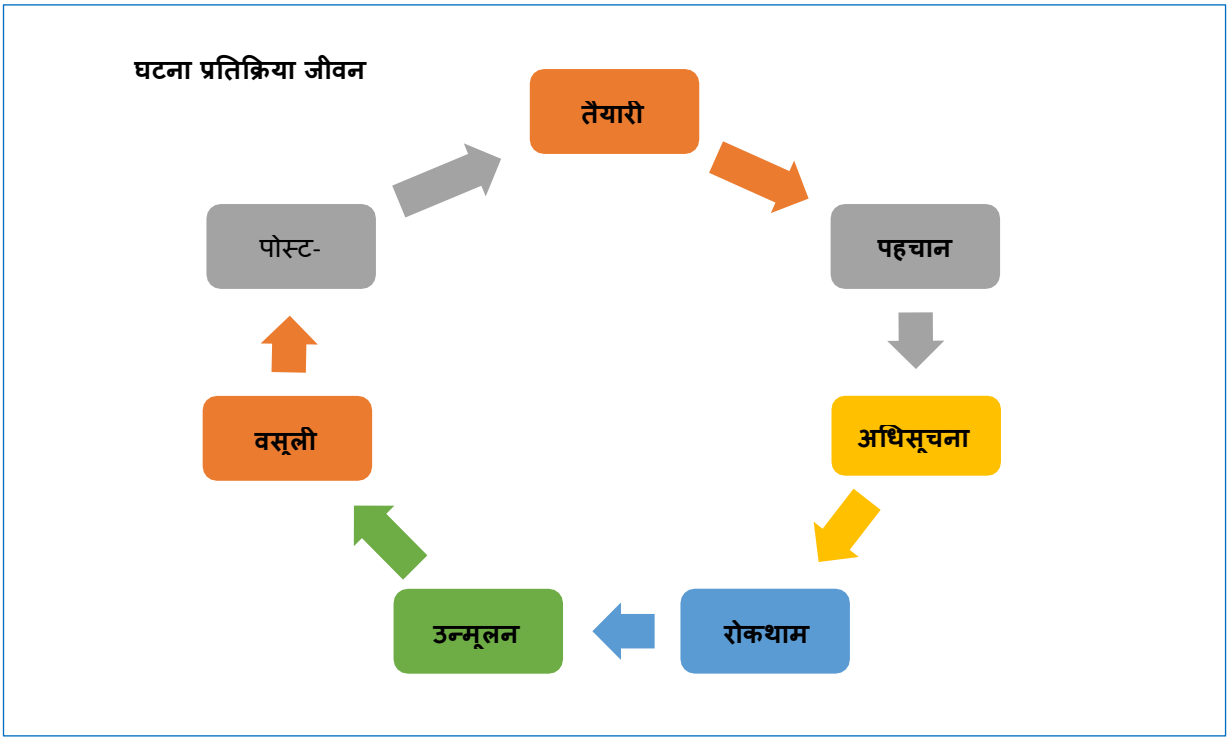
यह दस्तावेज़ साइबर सुरक्षा और डेटा उल्लंघन की घटनाओं पर सुसंगत और प्रभावी तरीके से प्रतिक्रिया देने के लिए दिशानिर्देश प्रदान करता है। यह योजना किसी घटना पर प्रतिक्रिया के लिए निर्धारित भूमिकाओं, ज़िम्मेदारियों और संचार के साधनों को स्थापित करती है। घटना की परिभाषा, प्रभाव और संभावित उदाहरण परिशिष्ट-ए में दिए गए हैं।

29.3 घटना प्रतिक्रिया जीवन चक्र

साइबर घटना प्रतिक्रिया प्रबंधन एक चक्रीय पैटर्न वाली सतत प्रक्रिया है। साइबर घटना प्रतिक्रिया योजना में शामिल विशिष्ट घटना प्रतिक्रिया प्रक्रिया तत्वों में शामिल हैं:

1. **तैयारी:** घटना प्रतिक्रिया क्षमताओं को बनाए रखने और सुधारने तथा यह सुनिश्चित करके घटनाओं को रोकने की सतत प्रक्रिया कि सिस्टम, नेटवर्क, अनुप्रयोग और डेटा हैंडलिंग प्रक्रियाएं पर्याप्त रूप से सुरक्षित हैं, तथा कर्मचारी जागरूकता प्रशिक्षण मौजूद है। आईआरटी के लिए अभ्यास (जिसे टेबल-टॉप अभ्यास भी कहा जाता है) समय-समय पर आयोजित किए जाते हैं, जहां अभ्यास सत्र में टीम के समक्ष विभिन्न घटना परिदृश्य प्रस्तुत किए जाते हैं।
2. **पहचान:** संदिग्ध घटनाओं की पुष्टि, लक्षण वर्णन, वर्गीकरण, श्रेणीकरण, दायरा निर्धारण और प्राथमिकता निर्धारण की प्रक्रिया।
3. **अधिसूचना:** किसी घटना के घटित होने पर आईआरटी सदस्यों को सचेत करना तथा घटना के दौरान संप्रेषण करना।
4. **रोकथाम:** वित्तीय और/या प्रतिष्ठा संबंधी हानि, सूचना की चोरी, या सेवा व्यवधान को न्यूनतम करना । आवश्यकतानुसार, घटकों और समाचार माध्यमों के साथ प्रारंभिक संचार करना।
5. **उन्मूलन:** खतरे को खत्म करना।
6. **वसूली:** कंप्यूटिंग सेवाओं को सामान्य परिचालन स्थिति में बहाल करना और व्यावसायिक गतिविधियों को शीघ्रता और सुरक्षित रूप से पुनः आरंभ करना। यदि आवश्यक हो, तो प्रतिष्ठा सुधार के उपाय और समाचार मीडिया अपडेट प्रदान करना। प्रभावित घटकों को ऋण निगरानी सेवाएँ प्रदान करना, या आवश्यकतानुसार अन्य सुधारात्मक उपाय प्रदान करना।
7. **घटना-पश्चात गतिविधियाँ:** समग्र प्रतिक्रिया प्रभावशीलता का आकलन और 'सीखे गए सबक' या शोषित कमज़ोरियों के शमन के माध्यम से सुधार के अवसरों की पहचान करना। घटना से प्राप्त सीखों को साइबर सुदृढ़ीकरण प्रयासों और प्रतिक्रिया योजना में, यथावश्यक, शामिल करना।

8. इन प्रक्रिया तत्वों को चित्र 1 में दर्शाया गया है, जो प्रक्रिया की बंद लूप प्रकृति को दर्शाता है, जिसमें किसी भी पूर्व घटना से प्राप्त सीख का उपयोग संभावित भविष्य की घटनाओं की रोकथाम और प्रतिक्रिया प्रक्रिया में सुधार के लिए किया जाता है।



आकृति 1

294 घटना प्रतिक्रिया टीम (आईआरटी)

कंपनी के कर्मचारियों, सलाहकारों और सेवा प्रदाताओं से बनी एक टीम घटना प्रतिक्रियाओं के समन्वय के लिए ज़िम्मेदार होगी और इसे घटना प्रतिक्रिया टीम (आईआरटी) के रूप में जाना जाएगा। इस टीम में प्राथमिक और द्वितीयक दोनों सदस्य होंगे। आईआरटी के प्राथमिक सदस्य, घटना की गंभीरता के अनुसार, आईआरटी की भागीदारी की आवश्यकता वाली किसी भी घटना में प्रथम प्रतिक्रियाकर्ता या सूचित सदस्य के रूप में कार्य करेंगे। सबसे गंभीर घटनाओं में पूरी आईआरटी को सूचित किया जाएगा और उन्हें शामिल किया जाएगा।

आवश्यकतानुसार, आईआरटी सदस्य किसी घटना के दौरान अतिरिक्त भूमिकाएँ निभा सकते हैं। संपर्क जानकारी, जिसमें प्राथमिक और द्वितीयक ईमेल पता, साथ ही कार्यालय और मोबाइल फ़ोन नंबर शामिल हैं, को बनाए रखा जाएगा और टीम को वितरित किया जाएगा। आईआरटी आवश्यकतानुसार किसी घटना के विश्लेषण, सुधार और पुनर्प्राप्ति प्रक्रियाओं के लिए अतिरिक्त कर्मचारियों, सलाहकारों या अन्य संसाधनों (जिन्हें अक्सर विषय विशेषज्ञ - एसएमई कहा जाता है) की सहायता लेगा। सूचना प्रौद्योगिकी (आईटी) कार्य उन तकनीकी विवरणों में महत्वपूर्ण भूमिका निभाता है जो किसी घटना का पता लगाने और प्रतिक्रिया में शामिल हो सकते हैं और इस संबंध में इसे एसएमई माना जा सकता है।

295 साइबर घटना प्रतिक्रिया टीम (आईआरटी):
प्राथमिक टीम सदस्य:

कार्यालय आदेश संख्या HUDCO/ITW/ERT/2023-24/01 या हडको द्वारा अपेक्षित इसके संशोधनों के अनुसार निम्नलिखित आपातकालीन प्रतिक्रिया दल की पहचान की गई।

क्रम सं.	भूमिका	नाम / पदनाम
1.	मुख्य आपातकालीन समन्वयक 1	
2.	मुख्य आपातकालीन समन्वयक 2	
3.	नेटवर्क समन्वयक/ सदस्य सचिव	
4.	सॉफ़्टवेयर समन्वयक	
5.	आईटी सुरक्षा समन्वयक	
6.	मानव संसाधन समन्वयक	
7.	प्रशासनिक सुविधाएँ	
8.	आईटी अवसंरचना समन्वयक	
9.	आपातकालीन प्रतिक्रिया कर्मचारी	

माध्यमिक टीम सदस्य:

सुरक्षा घटना निगरानी विक्रेता और/या कंप्यूटर फोरेंसिक विक्रेता:

- एसओसी एडमिन | हडको डेटा सेंटर
- जनसंपर्क विभाग प्रभारी
- साइबर बीमा प्रदाता - टाटा एआईजी

29.6 घटना प्रतिक्रिया प्रक्रिया विवरण

घटना प्रतिक्रिया के विस्तृत चरण और सामान्य समय नीचे दिए गए हैं।

प्रक्रिया चरण और अनुमानित समय	प्रक्रिया विवरण चरण	शामिल पार्टियाँ
पहचान (घंटे)	1. पहचान करें और पुष्टि करें कि संदिग्ध या रिपोर्ट की गई घटना घटित हुई है और क्या दुर्भावनापूर्ण गतिविधि अभी भी जारी है। 2. घटना के प्रकार, प्रभाव और गंभीरता का निर्धारण करें 3. बुनियादी और विवेकपूर्ण रोकथाम कदम उठाएँ।	आईटी और एसओसी निगरानी सेवा प्रदाता
अधिसूचना (घंटे - 1 दिन)	1. घटना की गंभीरता के आधार पर आईआरटी को सूचित या सक्रिय करें, तथा घटना के प्रकार, प्रभाव और विवरण को, जहां तक ज्ञात हो, उपलब्ध कराएं। 2. रोकथाम, उन्मूलन और पुनर्प्राप्ति प्रक्रियाओं में विषय वस्तु विशेषज्ञों (एसएमई) की भागीदारी की आवश्यकता का निर्धारण करें।	आईटी और आईआरटी

रोकथाम (घंटे-2 दिन)	1. किसी भी चल रही दुर्भावनापूर्ण गतिविधि को रोकने या पिछली दुर्भावनापूर्ण गतिविधि की पुनरावृत्ति को रोकने के लिए तत्काल कदम उठाएं। 2. यदि आवश्यक हो, तो सार्वजनिक वेबसाइटों को पुनर्निर्देशित करें। आवश्यकतानुसार प्रारंभिक जनसंपर्क और अन्य प्रतिक्रियाएँ प्रदान करें।	आईआरटी, आईटी, एसएमई
उन्मूलन (दिन - सप्ताह)	1. खतरे और संबंधित दुर्भावनापूर्ण गतिविधि का पूर्ण तकनीकी समाधान प्रदान करें। 2. जनसंपर्क, अधिसूचना और विधिक मुद्दों को संबोधित करें।	आईटी, आईआरटी, एसएमई
वसूली (सप्ताह - महीने)	1. किसी भी व्यावसायिक प्रक्रिया में व्यवधान को दूर करना और सामान्य परिचालन को पुनः प्राप्त करना। 2. यदि आवश्यक हो तो दीर्घकालिक जनसंपर्क या विधिक मुद्दों को संबोधित करें, और किसी भी घटक उपाय को लागू करें।	एसएमई, आईआरटी
घटना के बाद (महीने)	1. घटना का औपचारिक दस्तावेजीकरण करें और सीख को संक्षेप में प्रस्तुत करें। 2. सीखी हुई बातों को भविष्य की तैयारी में लागू करें।	आईआरटी

297 तैयारी

- **सिस्टम इन्वेंटरी** : महत्वपूर्ण प्रणालियों, डेटा, अनुप्रयोगों और निर्भरताओं की अद्यतन सूची बनाए रखें, ताकि उन परिसंपत्तियों की स्पष्ट समझ सुनिश्चित हो सके, जिन्हें संरक्षण की आवश्यकता है।
- **खतरे और जोखिम** की **पहचान** : आंतरिक और बाहरी कारकों पर विचार करते हुए, संगठन के संचालन के लिए संभावित खतरों, कमजोरियों और जोखिमों की पहचान करें।
- **निवारक उपाय** : अनधिकृत एक्सेस और साइबर खतरों से डेटा और प्रणालियों की सुरक्षा के लिए फायरवॉल, घुसपैठ का पता लगाने और रोकथाम प्रणाली (आईडीएस/आईपीएस), सुरक्षित एक्सेस नियंत्रण और एन्क्रिप्शन जैसे मजबूत निवारक उपायों को लागू करें।
- **नीतियों और प्रशिक्षण** : सुरक्षा नीतियां स्थापित करें और जागरूकता और तैयारी बढ़ाने के लिए कर्मचारियों को नियमित प्रशिक्षण प्रदान करें।
- **नियमित अद्यतन** : सुनिश्चित करें कि सिस्टम, सॉफ्टवेयर और निवारक उपकरण नियमित रूप से अद्यतन किए जाते हैं और ज्ञात कमजोरियों को दूर करने के लिए पैच किए जाते हैं।

298 घटना घटित होना और जागरूकता

किसी घटना के बारे में जिस प्रकार पता चलता है उसकी प्रतिक्रिया प्रक्रिया और उसकी तात्कालिकता पर प्रभाव पड़ता है। हमें किसी घटना की जानकारी कर्मचारियों/एसओसी टीम/तकनीकी प्रदाताओं/तीसरे पक्ष के मुखबिर के ज़रिए मिलती है।

299 घटना प्रतिक्रिया उपकरण

हडको को दुर्घटनाओं के प्रभावी प्रबंधन के लिए आवश्यक उपकरणों और संसाधनों की तैयारी सुनिश्चित करनी चाहिए। जिसमें शामिल हैं:

- **फोरेंसिक उपकरण** : घटनाओं के मूल कारण की पहचान करने के लिए डेटा की जांच, संग्रह और विश्लेषण के लिए उपकरणों/सेवा प्रदाताओं के साथ टीमों को सुसज्जित करना।

- **संचार प्रणालियाँ** : घटना प्रतिक्रिया और पुनर्प्राप्ति के दौरान स्पष्ट समन्वय सुनिश्चित करने के लिए सुरक्षित और विश्वसनीय संचार चैनल स्थापित करें।
- **पुनर्प्राप्ति** प्रणाली : परिचालन को शीघ्रता से बहाल करने और व्यवधानों को न्यूनतम करने के लिए मजबूत प्रणालियों और प्रक्रियाओं को लागू करें, जिसमें बैकअप समाधान, आपदा पुनर्प्राप्ति योजनाएं और सिस्टम पुनर्स्थापना उपकरण शामिल हैं।

29.10 घटना की पहचान

- वास्तविक समय में विसंगतियों और संभावित सुरक्षा उल्लंघनों का पता लगाने के लिए उन्नत निगरानी उपकरण और प्रणालियाँ लागू करें।
- घटनाओं की गंभीरता का आकलन करने और उनके प्रभाव के आधार पर प्रतिक्रिया प्रयासों को प्राथमिकता देने के लिए एक स्तरीय वर्गीकरण प्रणाली स्थापित करें।
- कर्मचारियों और बाहरी शेयरधारकों के लिए घटनाओं की तुरंत रिपोर्ट करने हेतु सरल, स्पष्ट और सुलभ तरीके विकसित करें।
- अनुपालन और प्रभावी घटना प्रबंधन सुनिश्चित करने के लिए विधिक प्रवर्तन, नियामक निकायों और अन्य प्रासंगिक प्राधिकरणों के साथ सहयोग करें।
- किसी घटना के दौरान समय पर, सुसंगत और सटीक संचार सुनिश्चित करने के लिए सार्वजनिक बयानों के लिए पूर्व-अनुमोदित टेम्पलेट और कौशलनीति तैयार करें।
- खतरों का प्रभावी ढंग से समाधान करने और उन्हें कम करने के लिए मान्यता प्राप्त साइबर सुरक्षा एजेंसियों और विधिक प्रवर्तन एजेंसियों के साथ मिलकर काम करें।
- उभरते खतरों और अनुपालन आवश्यकताओं के अनुरूप बने रहने के लिए इन उपायों को नियमित रूप से अद्यतन और परिष्कृत करें।

29.11 रोकथाम

- घटना को नेटवर्क में और अधिक फैलने से रोकने के लिए प्रभावित प्रणालियों की पहचान और उन्हें अलग करें।
- घटना के तत्काल प्रभाव को कम करने और संचालन को स्थिर करने के लिए अल्पकालिक उपायों को लागू करें।
- विधिक और फोरेंसिक दिशानिर्देशों का पालन करते हुए साक्ष्य एकत्रित, संरक्षित और दस्तावेजीकरण करें ताकि यह सुनिश्चित हो सके कि यह संभावित विधिक कार्यवाई में स्वीकार्य है।
- स्थायी समाधान की योजना बनाएं और उसे लागू करें जो घटना के मूल कारण को संबोधित करें, साथ ही महत्वपूर्ण सेवाओं में व्यवधान को न्यूनतम करें और व्यवसाय की निरंतरता सुनिश्चित करें।

29.12 उन्मूलन

यह चरण घटना के मूल कारण को दूर करने और यह सुनिश्चित करने पर केंद्रित है कि प्रणालियाँ सुरक्षित और स्थिर हैं। इसमें शामिल हैं:

- हमले के मूल का विश्लेषण और निर्धारण करें, जिसमें यह कैसे हुआ और कौन सी प्रणालियाँ प्रभावित हुईं।
- प्रभावित सिस्टम से हमलावर द्वारा छोड़े गए किसी भी दुर्भावनापूर्ण कोड, अनधिकृत सॉफ़्टवेयर या कलाकृतियों को हटा दें।
- हमले के दौरान शोषण की गई कमजोरियों को दूर करने के लिए आवश्यक अपडेट, पैच या कॉन्फ़िगरेशन परिवर्तन लागू करें ताकि पुनरावृत्ति को रोका जा सके।
- यह सुनिश्चित करने के लिए गहन समीक्षा करें कि सभी प्रभावित सिस्टम और डेटा को उनकी सुरक्षित और इच्छित स्थिति में बहाल कर दिया गया है, तथा वे किसी भी खतरे से मुक्त हैं।

29.13 रिकवरी

- डेटा अखंडता सुनिश्चित करने और किसी भी अवशिष्ट खतरे को समाप्त करने के लिए स्वच्छ, सत्यापित बैकअप का उपयोग करके प्रभावित सिस्टम का पुनर्निर्माण या पुनर्स्थापना करें।
- सिस्टम को पूर्णतः चालू करने से पहले यह पुष्टि कर लें कि वे सुरक्षित रूप से काम कर रहे हैं और अपेक्षा के अनुरूप प्रदर्शन कर रहे हैं।
- धीरे-धीरे चरणों में सिस्टम को ऑनलाइन वापस लाएं, जिससे प्रत्येक चरण के दौरान स्थिरता, प्रदर्शन और सुरक्षा की सावधानीपूर्वक निगरानी की जा सके।
- किसी भी लंबित कमजोरियों या समस्याओं का पता लगाने के लिए पुनर्स्थापित प्रणालियों का निरंतर मूल्यांकन करें, जिससे पूर्ण पुनर्प्राप्ति सुनिश्चित हो सके।

29.14 घटना के बाद का विश्लेषण

किसी घटना के बाद, घटना की प्रकृति और प्रभाव का मूल्यांकन करने, घटना प्रतिक्रिया प्रक्रिया की प्रभावशीलता का आकलन करने और प्रतिक्रिया के दौरान टीम के प्रदर्शन का विश्लेषण करने के लिए एक विस्तृत समीक्षा करें। घटना प्रतिक्रिया योजना (आईआरपी) को बेहतर बनाने और भविष्य की प्रतिक्रियाओं को मज़बूत बनाने के लिए प्रमुख अंतर्दृष्टि, सीखे गए सबक और पहचानी गई कमियों का दस्तावेज़ीकरण करें। आवश्यक रिपोर्ट तैयार करके और संबंधित शेयरधारकों के साथ निष्कर्ष साझा करके नियामक आवश्यकताओं और आंतरिक नीतियों का अनुपालन सुनिश्चित करें।

30 एजेंसियों को घटनाओं के प्रकार और विवरण सूचित करना

30.1 सीईआरटी-आईएन को घटनाओं की रिपोर्ट

हडको घटना के 6 घंटे के भीतर साइबर घटना की रिपोर्ट करेगा, जिसमें निम्नलिखित शामिल हो सकते हैं: -

- महत्वपूर्ण नेटवर्क/प्रणालियों की लक्षित स्कैनिंग/जांच।
- महत्वपूर्ण प्रणालियों/सूचनाओं से समझौता
- आईटी सिस्टम/डेटा तक अनधिकृत एक्सेस
- वेबसाइट को विकृत करना या वेबसाइट में घुसपैठ करना और अनधिकृत परिवर्तन जैसे दुर्भावनापूर्ण कोड, बाहरी वेबसाइटों के लिंक डालना आदि।
- उचित गंभीरता के दुर्भावनापूर्ण कोड हमले जैसे वायरस/वर्म/ट्रोजन/बॉट्स/स्पाइवेयर/रैंसमवेयर का प्रसार।
- डेटाबेस, मेल और डीएनएस जैसे सर्वरों और राउटर vii जैसे नेटवर्क उपकरणों पर हमला, पहचान की चोरी, स्पूफिंग और फ़िशिंग हमले
- सेवा अस्वीकार (DoS) और वितरित सेवा अस्वीकार (DDoS) हमले
- वायरलेस नेटवर्क पर हमले
- ई-गवर्नेंस, ई-कॉमर्स आदि जैसे अनुप्रयोगों पर हमले।
- डेटा उल्लंघन
- डेटा लीक
- इंटरनेट ऑफ थिंग्स (IoT) उपकरणों और संबंधित प्रणालियों, नेटवर्क, सॉफ्टवेयर, सर्वर पर हमले
- डिजिटल भुगतान प्रणालियों को प्रभावित करने वाले हमले या घटनाएं
- दुर्भावनापूर्ण मोबाइल ऐप्स के माध्यम से हमले
- नकली मोबाइल ऐप्स
- सोशल मीडिया अकाउंट तक अनधिकृत एक्सेस
- क्लाउड कंप्यूटिंग सिस्टम/सर्वर/सॉफ्टवेयर/एप्लिकेशन को प्रभावित करने वाले हमले या दुर्भावनापूर्ण/संदिग्ध गतिविधियाँ

- बिग डेटा, ब्लॉक चेन, वर्चुअल एसेट्स, वर्चुअल एसेट्स एक्सचेंज, कस्टोडियन वॉलेट्स, रोबोटिक्स से संबंधित सिस्टम/सर्वर/नेटवर्क/सॉफ्टवेयर/एप्लिकेशन को प्रभावित करने वाले हमले या दुर्भावनापूर्ण/संदिग्ध गतिविधियाँ,
- आर्टिफिशियल इंटेलिजेंस और मशीन लर्निंग से संबंधित सिस्टम/सर्वर/सॉफ्टवेयर/एप्लिकेशन को प्रभावित करने वाले हमले या दुर्भावनापूर्ण/संदिग्ध गतिविधियाँ।

संबंधित एजेंसियों के संपर्क विवरण निम्नलिखित हैं:

1) CERT- में:

साइबर सुरक्षा घटनाओं की रिपोर्ट CERT-In को दी जाएगी
वेबसाइट: https://www.cert-in.org.in
ईमेल: incident@cert-in.org.in
संपर्क नंबर: 011-24368551

2) भारतीय साइबर क्राइम समन्वय केंद्र (आई4सी)

साइबर धोखाधड़ी और अपराध की रिपोर्ट करने के लिए, गृह मंत्रालय द्वारा स्थापित **IHC** को रिपोर्ट करें ।
मंत्रालय की वेबसाइट: https://www.cybercrime.gov.in
फ़ोन: 1930

निम्नलिखित घटनाओं की गंभीरता के स्तर के आधार पर जानकारी दी जानी चाहिए:

घटना का प्रकार	विवरण का प्रकार	गंभीरता स्तर (5: अधिकांश गंभीर)	घटना प्रतिक्रिया
सेवा अस्वीकार (DoS), वितरित डीओएस (डीडीओएस), रैंसमवेयर हमला, अतिक्रमण	एक ऐसा हमला जो संसाधनों को समाप्त करके नेटवर्क, सिस्टम या अनुप्रयोगों की सामान्य अधिकृत कार्यक्षमता को सफलतापूर्वक रोकता या बिगाड़ता है।	5	आईटी विभाग, आईआरटी के संबंधित सदस्यों, प्राथमिक और माध्यमिक टीम के छोटे और मध्यम उद्यमों द्वारा समन्वित सुधार। आगे की फोरेंसिक जाँच और संभावित कानूनी परामर्श के लिए, यदि व्यक्तिगत पहचान उल्लंघन होता है, तो CERT-In और I4C कानूनी परामर्शदाता को सूचित करें।
डेटा उल्लंघन/डेटा लीक	आंतरिक डेटा उल्लंघन/लीक या ईआरपी डेटा	4	
अनधिकृत एक्सेस	जब कोई व्यक्ति या संस्था बिना अनुमति के कंपनी के नेटवर्क, सिस्टम, एप्लिकेशन, डेटा या अन्य संसाधन तक तार्किक या भौतिक एक्सेस प्राप्त कर लेती है।	4	

वेबसाइट साइबर घटना	वेबसाइट को ख़राब करना या उसमें घुसपैठ करना और अनधिकृत परिवर्तन जैसे दुर्भावनापूर्ण कोड डालना, बाहरी वेबसाइटों के लिंक डालना	4	
संदिग्ध PII उल्लंघन	1. ऐसी घटना जिसमें यह संदेह हो कि व्यक्तिगत पहचान योग्य जानकारी (PII) तक एक्सेस प्राप्त कर ली गई है 2.इसमें संवेदनशील जानकारी (PII नहीं) की संदिग्ध हानि शामिल है जो अनधिकृत एक्सेस, दुर्भावनापूर्ण कोड या अनुचित/अनुचित उपयोग के कारण हुई हो	3	
फ़िशिंग ई-मेल हमला	ई-मेल फ़िशिंग हमले के माध्यम से डेटा समझौता	3	ई-मेल सुरक्षा समाधान द्वारा नियंत्रित किया जाएगा
दुर्भावनापूर्ण कोड	दुर्भावनापूर्ण सॉफ़्टवेयर (जैसे, वायरस, वर्म, ट्रोजन हॉर्स, या अन्य कोड-आधारित दुर्भावनापूर्ण इकाई) जो किसी ऑपरेटिंग सिस्टम या एप्लिकेशन को संक्रमित करता है।	2	आईटी और एसएमई द्वारा समन्वित सुधार, आवश्यक कार्रवाई के लिए आईआरटी के संबंधित सदस्यों को सूचित किया जाएगा
किसी एकल व्यक्ति/ व्यक्तियों के समूह के डेटा या सेवाओं को प्रभावित करता है, जिसमें कोई संवेदनशील डेटा नहीं है	वायरस आदि से संक्रमित कंप्यूटर जिनमें कोई संवेदनशील डेटा नहीं है	1	सुधार और भविष्य निवारण पर ध्यान
बहुत कम या अनिर्धारित फोकस, उत्पत्ति और/या प्रभाव की घटनाएँ	खराब कंप्यूटर को सिस्टम एक्सेस लॉग, AV स्कैन या अन्य मरम्मत की आवश्यकता होती है।	0	हार्डवेयर टीम को द्वितीयक टीम द्वारा सूचित किया जाएगा

302 जानकारी रिकॉर्डिंग

किसी घटना के दौरान सूचना का अभिलेखन अत्यंत महत्वपूर्ण है, न केवल प्रभावी रोकथाम और उन्मूलन प्रयासों के लिए, बल्कि घटना के बाद सीखे गए सबक के लिए भी, और अपराधियों के विरुद्ध होने वाली किसी भी विधिक कार्रवाई हेतु भी। आईआरटी का प्रत्येक सदस्य परिशिष्ट बी में दिए गए आईआरटी घटना अभिलेख प्रपत्र का उपयोग करके, घटना के दौरान अपने कार्यों और निष्कर्षों के बारे में सूचना और तिथिक्रमानुसार संदर्भों को अभिलेखित करने के लिए उत्तरदायी होगा।

परिशिष्ट-ए
घटना प्रभाव परिभाषाएं

सुरक्षा उद्देश्य	सामान्य विवरण	संभावना प्रभाव उदाहरण		
		कम	मध्यम	उच्च
गोपनीयता: व्यक्तिगत गोपनीयता और मालिकाना संबंधी जानकारी की सुरक्षा के साधनों सहित सूचना तक एक्सेस और प्रकटीकरण पर प्रतिबंधों को बनाए रखना।	सूचना के अनधिकृत प्रकटीकरण से संगठनात्मक संचालन, संगठनात्मक परिसंपत्तियों या व्यक्तियों पर निम्नलिखित प्रतिकूल प्रभाव पड़ने की उम्मीद की जा सकती है।	एक या कई उपयोगकर्ताओं या कंप्यूटरों तक सीमित, आसान उपचार के साथ	उपयोगकर्ताओं के एक समूह को शामिल करना या प्रभावित करना, जिसके परिणामस्वरूप मालिकाना वाली जानकारी तक एक्सेस हो। सीमित या कोई बाहरी जोखिम नहीं।	बाहरी जोखिम के कारण मालिकाना जानकारी का गंभीर उल्लंघन।
अखंडता: सूचना के अनुचित संशोधन या विनाश से सुरक्षा; इसमें सूचना की अस्वीकृति और प्रामाणिकता सुनिश्चित करना शामिल है।	सूचना के अनधिकृत संशोधन या विनाश से संगठनात्मक संचालन, संगठनात्मक परिसंपत्तियों या व्यक्तियों पर निम्नलिखित प्रतिकूल प्रभाव पड़ने की उम्मीद की जा सकती है।	कंपनी डेटा में अनजाने या गैर-दुर्भावनापूर्ण परिवर्तन या विलोपन, जिसका आसानी से निवारण किया जा सकता है।	दुर्भावनापूर्ण या लापरवाहीपूर्ण प्रकृति का एक चल रहा अनुचित डेटा परिवर्तन कार्य (या कार्यों की श्रृंखला) जिसका मध्यम व्यावसायिक प्रभाव होगा।	कंपनी के डेटा में दुर्भावनापूर्ण या अवरोधक प्रकृति का बड़े पैमाने पर परिवर्तन या विनाश।
उपलब्धता: सूचना प्रणालियों तक समय पर और विश्वसनीय एक्सेस एवं उपयोग सुनिश्चित करना।	सूचना या सूचना प्रणाली तक एक्सेस या उपयोग में व्यवधान से संगठनात्मक संचालन, संगठनात्मक परिसंपत्तियों या व्यक्तियों पर निम्नलिखित प्रतिकूल प्रभाव पड़ने की उम्मीद की जा सकती है।	सीमित समय के लिए सीमित संख्या में उपयोगकर्ताओं को प्रभावित करने वाली मामूली रुकावट या दुर्गमता (< 2 घंटे)	किसी प्राथमिक व्यवसाय प्रणाली का व्यापक रूप से बाधित होना या 2 घंटे से अधिक, लेकिन एक दिन से कम समय तक एक्सेस से बाहर रहना	कंपनी की व्यावसायिक प्रणालियों में एक दिन या उससे अधिक समय तक गंभीर व्यवधान या अनुपलब्धता।

परिशिष्ट- बी

आईआरटी घटना अभिलेख रूप

दिनांक/समय	विवरण

घटना_____

खोज तारीख: _____

रिकॉर्डेड द्वारा: _____ पृष्ठों का _____पृष्ठ_____

CERT-घटना रिपोर्ट प्रपत्र में

Incident Reporting Form

Form to report Incidents to CERT-In				
For official use only:		Incident Tracking Number : CERTIn-xxxxxx		
1. Contact Information for this Incident:				
Name:	Organization:		Title:	
Phone / Fax No:	Mobile:		Email:	
Address:				
2. Sector : (Please tick the appropriate choices)				
Government Financial Power	Transportation Manufacturing Health	Telecommunications Academia Petroleum	InfoTech Other _____	
3. Physical Location of Affected Computer/ Network and name of ISP.				
4. Date and Time Incident Occurred:				
Date:		Time:		
5. Is the affected system/network critical to the organization's mission? (Yes / No). Details.				
6. Information of Affected System:				
IP Address:	Computer/ Host Name:	Operating System (incl. Ver./ release No.)	Last Patched/ Updated	Hardware Vendor/ Model
7. Type of Incident:				
Phishing Network scanning /Probing Break-in/Root Compromise Virus/Malicious Code Website Defacement System Misuse	Spam Bot/Botnet Email Spoofing Denial of Service(DoS) Distributed Denial of Service(DDoS) User Account Compromise	Website Intrusion Social Engineering Technical Vulnerability IP Spoofing Other_____		
8. Description of Incident:				

Incident Reporting Form

9. Unusual behavior/symptoms (Tick the symptoms)	
System crashes New user accounts/ Accounting discrepancies Failed or successful social engineering attempts Unexplained, poor system performance Unaccounted for changes in the DNS tables, router rules, or firewall rules Unexplained elevation or use of privileges Operation of a program or sniffer device to capture network traffic; An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user A system alarm or similar indication from an intrusion detection tool Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server	Anomalies Suspicious probes Suspicious browsing New files Changes in file lengths or dates Attempts to write to system Data modification or deletion Denial of service Door knob rattling Unusual time of usage Unusual usage patterns Unusual log file entries Presence of new setuid or setgid files Changes in system directories and files Presence of cracking utilities Activity during non-working hours or holidays Other (Please specify)

10. Has this problem been experienced earlier? If yes, details.

12. Agencies notified?			
Law Enforcement	Private Agency	Affected Product Vendor	Other_____

11. When and How was the incident detected:

13. Additional Information: (Include any other details noticed, relevant to the Security Incident.)	
Whether log being submitted	Mode of submission:

OPTIONAL INFORMATION

14. IP Address of Apparent or Suspected Source:	
Source IP address:	Other information available:

15. Security Infrastructure in place:				
	Name	OS	Version/Release	Last Patched/Updated
Name OS Version/Release Last Patched / Updated				
Anti-Virus				
Intrusion Detection/Prevention Systems				
Security Auditing Tools				
Secure Remote Access/Authorization Tools				
Access Control List				
Packet Filtering/Firewall				
Others				

Incident Reporting Form

16. How Many Host(s) are Affected		
1 to 10	10 to 100	More than 100
17. Actions taken to mitigate the intrusion/attack:		
No action taken System Binaries checked	Log Files examined System(s) disconnected form network	Restored with a good backup Other_____
Please fill all mandatory fields and try to provide optional details for early resolution of the Security Incident		
Mail/Fax this Form to: CERT-In, Electronics Niketan, CGO Complex, New Delhi 110003 Fax:+91-11-24368546 or email at: incident@cert-in.org.in		

परिशिष्ट- सी
एम्स साइबर घटना उपयोग मामला

घटना - एम्स सर्वर पर रैनसमवेयर हमला।

हमले के प्रभाव:

निम्नलिखित सभी ऑनलाइन सेवाएँ 19 दिनों के लिए बाधित रहेंगी

- स्मार्ट बिलिंग
- रिपोर्ट जनरेशन
- अपॉइंटमेंट बुकिंग
- पेशेंट आउट बिलिंग
- पेशेंट पंजीकरण

हमला कैसे होता है:

- एम्स में कुल 40 भौतिक सर्वर और 100 वर्चुअल सर्वर मौजूद हैं और एनआईसी द्वारा होस्ट किए जाते हैं।
- इनमें से पाँच सर्वर हमलावरों द्वारा हैक किए गए थे। कई सिस्टम रैंसमवेयर द्वारा एन्क्रिप्ट किए गए थे। कई मरीज़ों का संवेदनशील डेटा, साथ ही वीआईपी डेटा और पूर्व प्रधानमंत्री की स्वास्थ्य रिपोर्ट भी हमलावरों के हाथ लग गई थी।

एम्स ने स्थिति को कैसे संभाला (नियंत्रण)-

23 नवंबर 2022 की सुबह एम्स की प्रणालियाँ बहुत धीमी हो गईं और कुछ समय बाद सभी प्रणालियाँ असामान्य रूप से कार्य करने लगीं और ऑनलाइन सेवाएँ बाधित हो गईं। एम्स की तकनीकी टीम ने एनआईसी और सर्ट-इन से संपर्क किया और उन्होंने परिदृश्य की जाँच शुरू की और पाया कि सभी फ़ाइलों के एक्सटेंशन अज्ञात प्रारूप में बदल दिए गए हैं, जो रैंसमवेयर हमलों के संकेत हैं, एजेंसियों द्वारा इसकी पुष्टि की गई। सभी प्रभावित प्रणालियों को अलग कर दिया गया और सभी उपकरणों को नेटवर्क से हटा दिया गया। साइबर फोरेंसिक, दिल्ली साइबर पुलिस और थर्ड-पार्टी कंपनियों जैसी जाँच एजेंसियों ने एम्स को साइबर आतंकवाद और जबरन वसूली के प्रभाव को बेअसर करने में मदद की। दिल्ली पुलिस ने आईटी एक्ट की धारा 66F के तहत साइबर आतंकवाद और जबरन वसूली के तहत एक प्राथमिकी दर्ज की है। Cert-IN, NIC और अन्य एजेंसियों द्वारा संयुक्त रूप से की गई जाँच में पाया गया कि एम्स ईमेल सेवा के लिए ज़िम्ब्रा नामक एक सॉफ़्टवेयर का उपयोग करता है। इस सॉफ़्टवेयर के पुराने संस्करण के कारण, हमलावर इसमें दुर्भावनापूर्ण रैंसमवेयर फ़ाइल डालने में सक्षम थे और इसे अंजाम दिया गया।

संकल्प-तकनीशियनों ने प्रभावित प्रणालियों को नेटवर्क से अलग कर दिया और जिम्ब्रा ईमेल सेवा संस्करण को अपडेट किया, फिर उन्होंने नए सर्वरों में पुनः होस्ट किया।

अंततः 12 दिसंबर को सभी ई-सेवाएं बहाल हो गईं और ठीक से काम करने लगीं।