IT BCP/DR POLICY

Document Code: HUDCO/ IT-Policies/2024/05
Document Classification: Internal
(Version 1.1)

HOUSING & URBAN DEVELOPMENT CORPORATION LIMITED
Core 7-A, HUDCO Bhawan, India Habitat Centre, Lodhi Road,
New Delhi 110003

Website: www.hudco.org.in CIN: L74899 DL1970GOI005276

This document is for the internal use of Housing & Urban Development Corporation Ltd. (HUDCO) only and is not intended for use by any other person or entity. The procedures followed to create this policy do not constitute an audit, financial statement review, or examination of HUDCO's internal controls, fraud detection, or compliance with laws and regulations. No opinions or assurances are provided regarding HUDCO's financial statements, internal controls, or compliance matters.

Version History

S. No.	Version No.	Prepared By	Proposed By	Approved By	Dated
1.	1.0	Deloitte Corporate Finance Services India	ED (IT)	HUDCO Board	08.01.2019
2.	1.1	AKS IT Services Pvt. Ltd.	ED (IT)	HUDCO Board	16.12.2024

Table of Contents

1. Introduction

Business continuity planning (BCP) is an organization’s preparation process to ensure that critical business functions will be available even under extraordinary circumstances. Effective BCP develops a roadmap for maintaining service levels, consistency and recoverability for daily activities. BCP can sometimes be conflated with disaster recovery; however, disaster recovery is a subset of BCP as not all business disruptions would be categorized as disasters.

The Business Continuity Management (‘BCM’) is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resiliency and the capacity for an effective response that safeguards the interest of its key stakeholders, reputation, brand and value creating activities.

Through a properly designed, implemented and maintained BCM Program, HUDCO will be prepared to respond to a disaster or crisis event. The detailed elements of a BCM Program help the business to recover its critical operations more efficiently in the event of any type of business disruption. As the IT applications are deployed in centralized environment, policy shall be enforced at corporate office level.

2. Purpose

The purpose of a Business Continuity Policy (BCP) is to ensure that HUDCO can continue essential functions during and after a disaster or disruption. Below are the key points outlining its purpose:

1. **Minimize Downtime:** Ensure continuity of critical business operations with minimal interruptions during emergencies.
2. **Risk Mitigation:** Identify potential risks and develop strategies to mitigate their impact on operations.
3. **Resource Availability:** Ensure the availability of essential resources (personnel, technology, data, and facilities) to maintain operations.
4. **Protect Assets:** Safeguard physical, digital, and intellectual assets from potential threats.
5. **Ensure Safety:** Protect employees, customers, and stakeholders by having clear safety protocols in place.
6. **Regulatory Compliance:** Meet legal and regulatory requirements related to business continuity and disaster recovery.
7. **Maintain Customer Confidence:** Demonstrate reliability and resilience to customers, thereby maintaining trust and loyalty.
8. **Safeguard Reputation:** Reduce the impact of disruptions on the organization's public image and credibility.
9. **Facilitate Recovery:** Provide a clear roadmap for restoring normal operations quickly and efficiently after an incident.
10. **Enable Adaptability:** Build organizational resilience to adapt to and recover from unforeseen events.

By proactively planning for disruptions, a BCP ensures the organization is prepared to handle crisis while maintaining essential services and mitigating risks.

3. Scope

This policy is applicable to all HUDCO management including full time & part time associates, contractors, Vendors and external consultants.

4. Objective of BCM Framework

- To minimize financial loss.
- To ensure safety of IT resources.
- To continue to serve employees, customers and counterparties during disaster.
- To minimize the negative effects disruptions can have on strategic plan reputation, operations, earnings, liquidity, credit quality, market position, and the institution's ability to remain in compliance with applicable laws and regulations.

5. Exceptions

There may be instances where there is a justifiable business need to perform actions that are in conflict with Business Continuity Planning Policy. Whenever for technical or business reasons, it is not possible to comply with this policy, a time bound waiver must be requested. The waiver needs to be approved by the ED(IT). All approved exceptions should be reviewed at least annually or as and when required. Any issue related to interpretation shall be approved by competent authority.

6. Business Continuity Management Overview

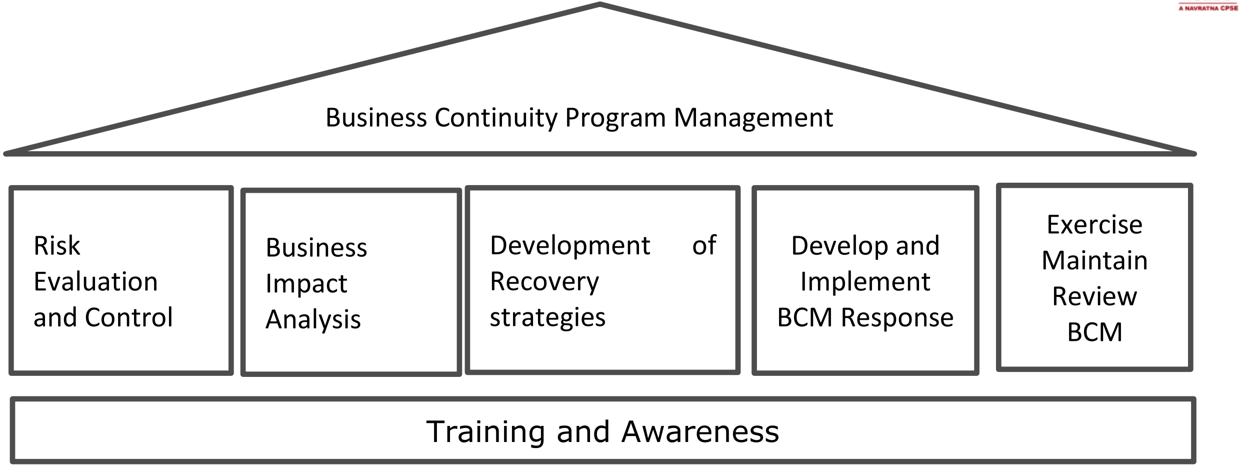
Business continuity Management requires development and implementation of strategies, plans, resources and actions to ensure the continued achievement of critical objectives in the event of a significant, untoward, crisis event.

BCM focuses on:

- Identifying dependencies/ vulnerabilities within organizations, especially those linked to the underlying processes creating value. Understanding, the impact of their non-availability over the time on the organization.
- Identify procedure to minimize impact on the overall value creation in case of a disaster.

7. Business Continuity Management Framework

Preparing HUDCO for a crisis involves building a framework that is both resilient to business disruptions and capable of an effective response to varying levels of interruptions and outages. The phases of the preparation process include risk evaluation and control, analysis of business impacts, development of recovery strategies, plan development and implementation, exercising and training. Adherence to the follow Department standards will prepare HUDCO for a crisis in a manner that complies with corporate policy and adheres to industry-preferred Business Continuity Management practices.


Business Continuity Program Management
Risk Evaluation and Control
Business Impact Analysis
Development of Recovery strategies
Develop and Implement BCM Response
Exercise Maintain Review BCM
Training and Awareness

8. Risk Evaluation and Control

A risk analysis determines the sources of conditions that can adversely affect HUDCO and its facilities in the case of a loss of critical resources, the damage such conditions can cause and the controls needed to prevent and minimize the effects of potential loss.

A risk analysis will be conducted annually (or in response to change within the organization or business environment) by the Business Continuity Planning Team. It is the responsibility of the respective coordinators to obtain the necessary internal and external resources to complete risk analysis. A risk analysis will be performed for all aspects of Business Area’s operations, including IT Infrastructure and Applications.

The follow Department triggers, will indicate that a re-evaluation of risk is required more frequently than the annual schedule:

- Occupation of a new building.
- Changes in physical surroundings (i.e. construction of buildings, city threats, etc.).
- New products or business partner relationships.
- Changes in network architecture.
- Changes in data center location and/or design.
- Significant new regulations.
- Significant process changes.

A common risk analysis methodology will be used across HUDCO to evaluate the probability of occurrence and possible impact of each potential risk. This methodology will provide a common method for information gathering, evaluation of probability and severity, an ongoing evaluation process, identification of physical, information security, legal and regulatory issues, and analysis of cost and benefits associated with a potential risk.

At a minimum, environmental, technological, operational, political, and legal and security risks from both internal and external sources will be identified. For each risk identified, the probability of occurrence and potential loss will be measured. The current controls and safeguards to prevent and/or minimize the effect of the risk and loss potential will be identified and assessed for effectiveness.

Specific controls that will be identified and assessed may include, but not be limited to:

- Physical location

- Physical infrastructure design
- Building security and access controls
- Personnel procedures
- Third-party contracts
- Information security (i.e. data center, network, hardware, operating system, application, database level security)
- Information backup and protection
- Preventive maintenance and equipment planning
- Redundant services (electricity, air conditioning, water, communications, equipment replacement and spares)

Those conducting risk analyses will identify and evaluate controls and enhancement options for risk mitigation. The controls should primarily be preventative in nature. Where preventive controls are not an option, the proper balance between detective and corrective controls will be implemented. The Business Area Leader will determine whether to avoid, transfer and/or accept risks and approve proposed investment in controls.

The BCM Leader will resolve conflicts for risk transfers and acceptance techniques that are deployed but conflict with the needs and impacts another business area.

Follow Department are the threats considered for Risk assessment:

Natural Hazards	Accidental Hazards
Earthquake	Fire
Hurricane	Equipment / IT Hardware Failure
Flood	Building/structure collapse
Pandemic Outbreak	
Intentional Acts	Infrastructure Related Threats
Bomb Threat	Power Disruption
Civil Disorder	Telecom / Internet Disruption
Denial of Service	Water Damage
Brute Force Attack	Low platform/VM/application performance
Malware	Data cannot be restored
Enemy attack, war	Poor network performance
Sabotage	
Crime	
External/Internal attacker attacking unpatched applications/systems	
External/Internal attacker attacking vulnerable applications/systems	
External/Internal attacker attacking obsolete platforms	
Privileged access	
Physical security breach	

9. Business Impact Analysis (BIA)

A Business Impact Analysis is a management level analysis which identifies the impacts of losing company resources, reputation of the organization; measures the effect of resource loss and escalating losses over time in order to provide senior management with reliable data upon which to base decisions on risk mitigation and continuity planning.

The Business Impact Analysis identifies the impacts resulting from disruptions and disaster scenarios that can affect the organization and the techniques that can be used to quantify and qualify such impacts. BIA is conducted to identify time-critical functions, recovery priorities, resources, and inter-dependencies so that recovery time objectives (RTO), recovery point objectives (RPO) and Maximum Tolerable Period of Disruption (MTPD) can be set.

HUDCO must plan and implement DR Site where all identified servers/applications must be hosted. HUDCO must record DR drill exercises activity records with achieved RPO/RTO. The DR Drill report shall be placed to IT Strategy Committee of the Board.

S.No.	Business Process and Service	Application/ System	Maximum Tolerable Downtime in Minutes, Hours, Days, Weeks	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)

Any major issues observed during the DR drill shall be resolved and tested again to ensure successful conduct of drill before the next cycle.

The DR testing shall involve switching over to the DR / alternate site and thus using it as the primary site for sufficiently long period where usual business operations of at least a full working day (including Beginning of Day to End of Day operations) are covered.

HUDCO shall regularly test the BCP / DR under different scenarios for possible types of contingencies, to ensure that it is up-to-date and effective.

HUDCO shall ensure that DR architecture and procedures are robust, meeting the defined RTO and RPO for any recovery operations in case of contingency.

HUDCO shall ensure BCP and DR capabilities in critical interconnected systems and networks including those of vendors and partners. HUDCO shall ensure demonstrated readiness through collaborative and co-ordinated resilience testing that meets the HUDCOs' RTO.

10. Develop Recovery Strategy

Recovery strategies are developed to mitigate the identified risk exposures and potential business impacts of disruptions. Strategies are selected and implemented according to business priorities and objectives.

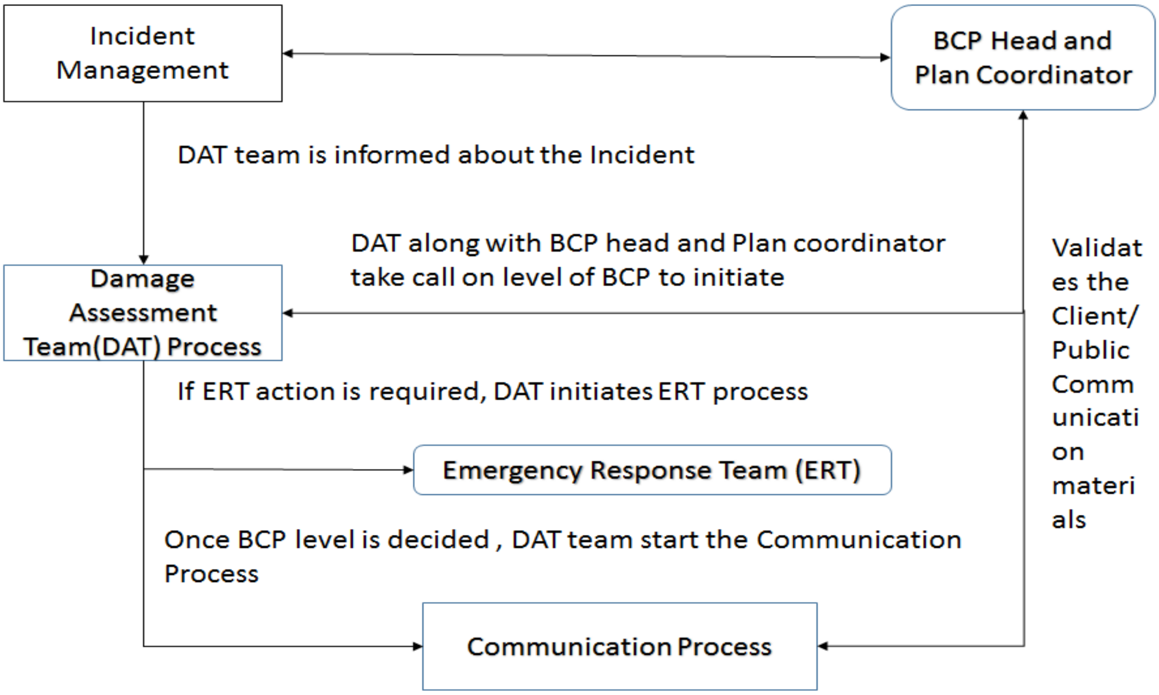
Table below outlines the brief descriptions of scenarios/ levels of BCP along with assumption and BCP activity.

Disaster Level	Disaster Description	BCP Activity
L1-a	HUDCO corporate office operations facility is unavailable due to either threats listed in Risk Assessment (RA) section or un-known threat.	If the extent of damage to the facility is of the nature that renders the facility unavailable for months, then all employees taking care of critical processes/activities will be allowed to work from home/alternate location and operate from there till the original facility is restored. Facilities team along with external vendors (if required) work towards restoring the original facility / IT Infrastructure. Once the facility / IT infrastructure is restored, the BCP coordinator and the BCP head are informed about it. All the employees are communicated of the restoration and shall start work from HUDCO corporate office and resume normal operations.
L1-b	HUDCO corporate office operations is available, however, power / telecom / data outage has rendered its operation non-functional.	Resources based at alternate location will take over the operation as well as each employee of HUDCO - corporate office that has laptops so they work from their home or from alternate location.
L1-c	HUDCO corporate office personnel are not available due to mass resignation/epidemic.	Resources based out at alternate location will take over the operations. During the unavailability of HUDCO corporate office personnel, alternate location resources will double up for the HUDCO Office resources and take over the work load.

11. BCM Plan Development and Response

Business Continuity plans are documented and implemented based on the recovery strategies that meet business needs.

Strategy & Activation Criteria


Incident Management
BCP Head and Plan Coordinator
DAT team is informed about the Incident
DAT along with BCP head and Plan coordinator take call on level of BCP to initiate
Validates the Client/ Public Communication materials
Damage Assessment Team(DAT) Process
If ERT action is required, DAT initiates ERT process
Emergency Response Team (ERT)
Once BCP level is decided , DAT team start the Communication Process
Communication Process

12. Incident Reporting

On first noticing the incident which may lead to disruption in operations, Incident Management team will immediately notify the Damage Assessment Coordinator, BCP coordinator and BCP Head.

General Evacuation Procedure

- Building occupants will be notified of the evacuation by the sound of the building fire alarm or by verbal instruction from building emergency staff.
- All occupants must leave the building immediately if the fire alarm is activated, or if directed to do so by building emergency staff.
- Building emergency staff will guide and assist the evacuation to the extent possible.
- All occupants should exit the building through the nearest safe exit or exit. Elevators should never be used in an emergency evacuation.
- If the nearest exit is obstructed by smoke, fire or other hazards, proceed to an alternate exit or exit stairwell.
- During stairwell evacuation, remove high heels, and hold on to the handrail. Allow enough room for others to enter the flow of traffic in the stairwell.

- Once outdoors all occupants should move to the assembly area, located in parking lots adjacent to the building.
- Emergency staff members should ensure that proper assistance has been summoned, if necessary, by calling the Fire / Police / Ambulance department etc.
- Once assembled, emergency staff will account for all occupants, in order to inform arriving emergency services if anyone is missing or possibly still inside the building.
- Building emergency staff will also inform arriving emergency personnel of information about the emergency in the building, including location of hazards and any problems known.
- Building occupants should not re-enter the building until cleared by emergency personnel.

13. Disaster Recovery Plan

13.1 Disaster Recovery Management

- Periodicity of DR drills for critical information systems shall be preferably on a half yearly basis and for other information systems, as per HUDCO's risk assessment.
- HUDCO should prioritize achieving minimal RTO (as approved by the HUDCO's ITSC) and a near zero RPO for critical information systems.
- In a scenario of non-zero RPO, HUDCO shall have a documented methodology for reconciliation of data while resuming operations from the alternate location.
- HUDCO shall ensure that the configurations of information systems and deployed security patches at the DC and DR are identical.

13.2 Near Disaster Recovery Site:

- Set up an off-site location to mirror the primary data center with critical infrastructure and failover capabilities.
- Ensure minimal downtime and quick service transition during emergencies.
- Identify and prioritize essential services (e.g., payroll, loan processing, ERP) in the IT strategy plan.
- Ensure these services are operational at the disaster recovery site.

14. Backup Policy

As per Backup policy, the following are stated -

- Frequency of all scheduled backups must be taken based on the criticality of the applications and their defined Recovery Point Objectives (RPO) mentioned in the Business Continuity Plan. The frequency of backup purely depends on the data to be backed up and the respective criticality of the application.
- The IT Department shall be responsible for setting up of backup process.
- Full database & Application backup shall be taken daily.
- HUDCO shall backup data and periodically restore such backed-up data to check its usability. The integrity of such backup data shall be preserved along with securing it from unauthorized access.

15. Critical Services Transfer Plan

All key processes identified from the Business Impact Analysis will be under direct scope of this activity. Every critical business and support services in HUDCO corporate office, will be transferred to the working facility in alternate location.

Information Technology Department will:

- Identify the critical resources and critical personnel which are required to lead the development activity.
- Personnel shortlisted as critical for the function will be trained on how to perform in the event of a disaster.
- Gather regular status updates from the personnel, Communicate and assure the client(s) of business continuity.

16. Emergency Response Plan

It is a standard set of procedures that address the initial reaction for the protection of life and the activities to ensure the safety of all personnel, as well as the activities required to mitigate the impact of an emergency and to work with emergency personnel to minimize or contain an emergency situation.

HUDCO will maintain a basic emergency kit for general use in the main administrative office. In an emergency evacuation, the kit will be transported by main office staff outdoors to the evacuation assembly area. The kit contains:

- A copy of this emergency plan (Emergency Response Plan section of the BCP), along with a current employee roster will be used in accounting for building personnel after an evacuation first aid supplies. In some emergencies, personnel may have to provide first aid to those with non-life-threatening injuries.
- Flashlights and extra batteries.
- Small emergency water and food supply.
- List of essential phone numbers, including phone numbers of key family members of all the employees.

17. Assembly Points

- Where the premises need to be evacuated, the emergency response plan identifies evacuation assembly points:
- In-front of HUDCO Corporate Office, Core-7A gate.

18. Information Security

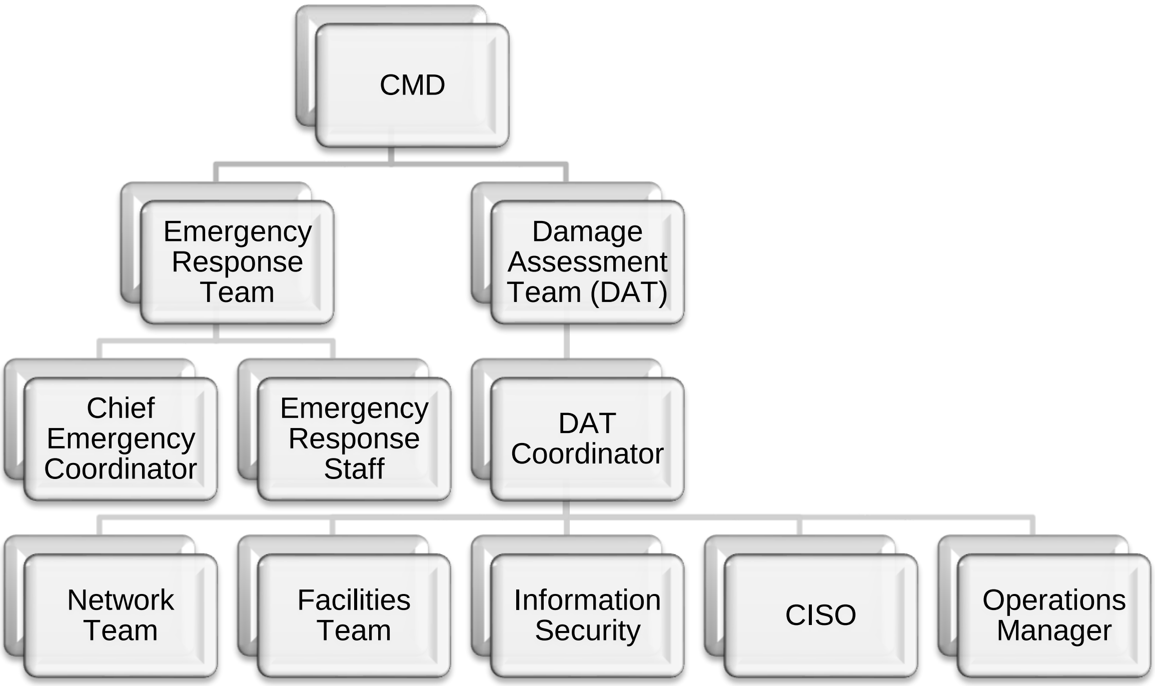
- In a disaster, all focus shall be on getting critical business processes back up and running. Whether the disaster is natural or manmade, it's all about recovering business operations as fast as possible, getting employees back to work, and avoiding costly downtime.
- In this scenario, generally information security is often far down on the list of considerations, but HUDCO understands that companies that overlook data protection provisions in their disaster recovery/business continuity plans risk may face double issue, a security breach on top of a recovery situation.
- HUDCO is committed to ensure that security policies are maintained in a recovery situation.

19. Communications and Public Information plan

- An emergency event may occur with or without prior warning. The communication process will be the same in either case. The manner in which personnel are notified depends on the type of emergency and whether the emergency occurs during or after normal business hours. Communication will be accomplished by phone, e-mail, word of mouth or cell phone.

- The first responder is to notify the BCP Head & BCP Coordinator. All known information will be relayed to the BCP Coordinator and BCP Head.
- The BCP Coordinator will contact the concerned personnel according to the ERT Team.
- Upon activation of the BCP, the Team Leads of hit site (i.e. site hit by disaster) will notify their team members.
- Communication Coordinator must ensure that all personnel have been notified not to release information and to refer requests to the organization's spokesperson.
- Advertise using appropriate media, as necessary.
- Contact clients as necessary and provide them with important information such as Nature of Disaster, Level of BCP declared i.e. Disaster Level L1 along with tentative impact on service delivery etc.

20. Business Continuity Management Structure



21. Roles and Responsibilities of Damage Assessment Team

- Assessing the current damage due to un-controlled/new threats.
- Initiating emergency response process.
- Deciding on the level of BCP applicable (i.e. L1 – a, L1 – b, L1 – c).
- The DAT is comprised of Team Leader of Network Team, Data Center Team, Facilities Team, Information Security Team, CISO etc. The Damage Assessment Coordinator will inform the BCP Head & BCP Coordinator of the damage assessment progress and report any issues.
- DAT will work closely with the BCP Coordinator during the damage assessment.

- After the completion of assessment, the DAT Coordinator will notify the BCP coordinator to relay the results. Based on available information, the BCP Head, BCP Coordinator and Damage Assessment Coordinator will determine the level of the contingency event (i.e. L1 – a, L1 – b, L1 – c). The level of the contingency event will determine if relocation is necessary. Based on damage assessment results, the communication coordinator will notify civil emergency personnel (e.g., fire, police) & relevant stakeholders, as appropriate.

22. Roles and Responsibilities of Emergency Response Team

22.1 Chief Emergency Coordinator

The Chief Emergency Coordinator oversees response to any emergency situation for the department. In the event of an emergency, the duties of this position include:

- During an evacuation, ensure that proper assistance has been summoned if necessary.
- Ensure that the emergency response kit is brought to the assembly area by a designated Staff member, including the employee roster.
- Ensure that emergency response staff initiate evacuation procedures, providing instructions to occupants.
- At the evacuation assembly area, receive status reports from emergency response staff. Ensure that response staff assesses head count, using the roster maintained in the emergency kit.
- Meet arriving emergency services personnel, providing information on location of the emergency, layout of the building, any problems requiring assistance, and location of personnel.
- Help to ensure that building occupants do not enter the building until cleared to do so by emergency services.
- If there are individuals in the building who require assistance in evacuation due to disability, ensure that assistance is provided.
- On an ongoing basis, ensure that this emergency plan is kept current.

22.2 Emergency Response Staff

- Each response staff member has been assigned responsibility for a designated zone of the building. Their assignment is to assist in coordinating response to an emergency, ensuring that appropriate initial action has been taken, including activation of the alarm system if necessary and summoning emergency assistance.
- Specific responsibilities during an emergency evacuation include:
- Make a quick check of your zone to ensure that everyone has been notified of the need to evacuate the building. Strongly advise all building occupants that they must leave the building immediately. This should be done quickly and in a manner that does not endanger your safety.
- Direct all building occupants not to use the elevator, but to proceed to the nearest stairwell. Direct them to exit the building and proceed to the assembly point in closest parking lot adjacent building.
- If the nearest stairwell is obstructed by smoke, fire, or other hazards, direct occupants to the alternate exit.
- If any occupant requires assistance in moving down the stairwell due to a disability, ensure that appropriate assistance is provided.
- Proceed to the evacuation assembly area and assess the personnel headcount for your zone.

- Provide a status report to the Chief Emergency Coordinator on any problems, including individuals who are missing and may still be in the building, any problems requiring immediate assistance by emergency services, and any disabled individuals who require evacuation assistance.
- Help to ensure that building occupants do not re-enter the building until cleared to do so by emergency services.
- Assist in disseminating emergency instructions or information.
- Assist in providing information to emergency services as they arrive.

23. Guidelines for BCP Teams for responding to emergency situations

23.1 Fire Safety Guidelines

Firefighting methods & preventive measures to be Admin Department

- Appropriate number of Class A, B, C fire extinguishers is placed at accessible places on the floor and its records are maintained. Responsibility: Admin
- All the Fire Extinguishers are inspected every month, and its record is maintained. Responsibility: Admin
- It is ensured that the following are displayed at all the suitable locations and its records are maintained
- Emergency Evacuation plans,
- Florescent Emergency Exit Sign Boards
- List of ERT members
  List of Emergency Telephone/ Mobile Numbers.
- ERT (Emergency Response Team) consisting of appropriate number of employees from different sections is made. It is ensured that all the members of ERT, security guards, Admin, HR are trained in Fire Fighting. The records are to be maintained.
- All the existing and new joiners are trained on Fire Safety Guidelines. The records are to be maintained.
- Fire Drill is done at least half yearly, and its records are to be maintained.
- A team of First Aid Trained Personnel (FATP) is made with appropriate number of employees from different sections.

23.2 In the event of fire break

- Raise the alarm. Respond to the alarm instantly. In the buildings where there is no fire alarm system, alert-building occupants by word of mouth.
- Call Admin Department or, HR Department.
- Provide the following information:
  - Your name and location
  - Location of fire
  - Details as requested
- Leave the building as quickly as possible. Don't Panic.
- No effort should be made to deal with the fire unless such action is compatible with the safety of all concerned. Wait for further instructions from Admin/ HR/ Emergency Response Teams ('ERT'). Follow instructions only from Admin/ HR/ ERTs as they have been trained in handling such situations.
- Do not try to save any valuables or work-related material as it may obstruct the evacuation process.
- Do not break windows or locked doors except the exit door unless instructed by Admin/ HR/ ERT.
- Do not use lifts/ elevator as the oxygen in the lift/ elevator shafts helps fire escalation. Use the nearest exit.

- Evacuate in an orderly but brisk manner. Follow the self-illuminating glow signs that lead to the emergency exit. If caught in dense smoke, take short breaths through your nose and crawl to the nearest emergency exit, as the air closest to the floor will be more breathable.
- Assist elderly people, physically disabled people only if you are in a position to do so.
- Be extremely cautious while opening any door. Feel for heat and keep the door in front of you for protection.
- Place a wet cloth, if available, along the bottom of the door to keep out smoke.
- If you are caught in a cabin, place a Save our Souls (SOS) sign in the window for the fire fighters to see. If your office windows are tinted, use a flashlight to attract attention. Never break a window, except at the behest of a fire.

23.3 After fire breaks out

- First Aid Trained Personnel (FATP) provides aid where appropriate. Seriously injured or burned victims should be provided professional medical assistance immediately.
- Stay out of the damaged premises. Return only when the Admin/ HR/ ERT inform it is safe.

23.4 HR responsibilities

- Manage the Assembly during fire
- Ensure all the entered employees have exited

23.5 Fire Drill

- Fire Drill is organized every quarterly and Admin maintains its record.
- HR readies the list of Employees present on the day of fire drill so that the Roll Call is correctly taken. The deviation report is made and reported to Admin/ management.
- HR makes the displays to help managing assembly.
- Admin take the note of the time of effective evacuation/ fire drill.
- A Fire Drill Effectiveness report is forwarded to IT Department.
- The report contains:
- ○ Deviation in the list of manpower
- ○ Effective Fire Drill Time
- ○ Discipline
- ○ Other information, if any.

23.6 Earthquake

The following procedures apply to major earthquakes that cause strong shaking:

- If indoors, drop, cover, and hold. Protect yourself from falling objects such as light fixtures, bookcases, cabinets, shelves, and other furniture that might slide or topple. Stay away from windows. If possible, get under a table or desk. Hold on and be prepared to move with it. If no shelter is available, seek cover against an interior wall and protect your head and neck with your arms.
- Do not stand in a doorway. The earthquake safety procedure of moving to a doorway is obsolete, and doorways offer no greater protection than any other area. In fact, some individuals have been injured while moving toward or standing in a doorway during an earthquake.
- If outside, move away from structures, power poles, or other possible hazards. Stay in an open area.

- During the shaking, do not run for exits or attempt to leave the building, since heavy objects or debris may be falling in your path.
- Do not use the elevators.
- When the shaking stops, check for injuries to personnel in your area. Do not attempt to move seriously injured persons unless they are in immediate danger. Render first aid assistance if required.
- Check the area for safety hazards such as building damage, fires, spills of flammable or combustible liquids, or leaks of flammable gases. If the area or building appears to be unsafe, begin evacuation procedures.
- Turn off electrical equipment and gas sources before evacuating if it is safe to do so.
- Exit the building and go to the assembly point to report on injuries, damage, and potentially hazardous conditions.
- Call ambulance to report any serious injuries or other immediate emergencies.
- Once you have exited the building, do not reenter until the building has been inspected by trained emergency personnel.

23.7 Power Outage

Response to a power outage will depend on the circumstances. If possible, information should be obtained from the Facilities Team on the extent and likely duration of the outage.

- Damage Assessment Team will assess the extent of the outage in your area and report status to the Chief Emergency Coordinator and BCP coordinator.
- Help persons in darkened work areas move to safety.
- Check elevators to determine if anyone is trapped inside. If so, immediately call for help; do not attempt to force open doors and rescue them. Wait for a qualified elevator mechanic.
- Unplug desktop computers, equipment, and appliances during the outage, especially if not connected to a surge protector.
- Shutdown any equipment or process that could be hazardous if the power suddenly returns.
- Request direction from the Chief Emergency Coordinator regarding whether to evacuate or stay in place.

23.8 Medical Emergencies

In the event of a medical emergency:

Call 102 to request assistance. Provide the following information:

- Building address and phone number
- Floor or room number
- Nature of injury
- Location of injured person
- Age of injured person
- Sex of injured person
- Current condition

- Any known medical history

In addition, notify the Chief Emergency Coordinator and Emergency Response Staff.

Remain with the person with the medical emergency. Do not move them unless they are in immediate danger of further injury.

23.9 Bomb Threat Procedures

- HUDCO personnel receiving telephoned bomb threats should get as much information as possible from the caller, using the form below, and report it immediately to the Police Department (100).
- Bomb threats received through the mail or by other means are also to be reported immediately to the Police Department (100).
- The Bomb Disposal Squad will assess the threat and advise building occupants if it is necessary to evacuate the building.
- If it is necessary to evacuate, the chief emergency coordinator along with emergency response staff will assemble all the building occupants in the parking lot and remain 300 feet away from the building until advised to return.

23.10 Emergency Evacuation for Persons with Disabilities

Questions to ask the caller to gather as much information as possible:

1. When is the bomb going to explode?
2. Where is the bomb right now?
3. What does it look like?
4. What kind of bomb is it?
5. What will cause it to explode?
6. Did you place the bomb?
7. Why?
8. What is your address?
9. What is your name?

This section provides a general guideline of evacuation procedures for persons with disabilities during fire and other building emergencies. Individuals with disabilities must identify their primary and secondary evacuation routes, and seek out colleagues who are willing to serve as evacuation assistants. Other personnel can help by becoming aware of others who may need assistance in an evacuation.

MOBILITY-IMPAIRED –WHEELCHAIR

In most buildings people will need to use stairways to reach building exits. Elevators cannot be used because they have been shown to be unsafe in an emergency.

For persons in wheelchairs located on the first floor, they may use building exits to the outside ground level. For disabled individuals on upper floors, it is not safe to attempt to move a wheelchair down a stairwell.

One effective approach to this situation is the following:

Stay in Place

Working with an evacuation assistant, select a room with an exterior window, a telephone, and a solid or fire-resistant door. Remain with the disabled person in this room, and send someone to the evacuation assembly area to notify emergency personnel of the location of the person in need of assistance. It is also possible to place the disabled person near a stairway landing to await assistance, although this area may not be protected from smoke and other hazards.

Fire Department personnel, who are trained in emergency rescue, can then enter the building and assist the person in exiting the building, either down the stairs or using the emergency elevator recall.

While staying in place, the wheelchair user should keep in contact with emergency services and reporting his or her location directly.

Stairway evacuation of wheelchair users should be conducted by trained professionals from the fire department. Only in situations of extreme danger should untrained people attempt to evacuate wheelchair users. If this must be attempted, one possibility is the following:

Person Cradle Carry

- Wait until other evacuees have moved down the stairwell.
- The two helpers stand on either side of the individual.
- They reach under the individual and lift them out in a cradle.
- Helpers control the descent by walking slowly and cautiously.

NEVER LEAVE A WHEELCHAIR IN A STAIRWELL.

- Office Chair Evacuation.
- Transfer the physically challenged individual to a sturdy office chair.
- One helper gently leans the chair backwards.
- The other helper faces the chair and holds onto the front legs of the chair. Both will lift the chair simultaneously.
- The helpers control the descent by bending their legs slowly and keeping their back straight.

MOBILITY IMPAIRED - NON-WHEELCHAIR

Persons with mobility impairments who are able to walk independently should be able to negotiate stairs in an emergency with minor assistance. The individual should wait until the heavy traffic has cleared on the stairwell before attempting to exit.

HEARING IMPAIRED

Persons with hearing impairments may not hear audio emergency alarms and will need to be alerted to emergency situations by other building occupants.

VISUALLY IMPAIRED

Most people with a visual impairment will be familiar with their immediate surroundings and frequently traveled routes. Since the emergency evacuation route may be different from the commonly traveled route, persons who are visually impaired may need assistance in evacuating. The assistant should offer his/her elbow to the individual with a visual impairment and guide him or her through the evacuation route. During the evacuation the assistant should communicate as necessary to ensure safe evacuation. Emergency response staff should assess the needs of any building occupants with special needs within their zone prior to an emergency. Ask if there are any employees who will need assistance in the event of an evacuation, and arrange for nearby individuals to serve as evacuation assistants.

24. Incident Reporting Contacts

HUDCO to maintain Incident reporting contact list.

S. No	Designation	Service/Department	Contact Number	Location

25. Emergency Services

Minimum Employee Requirement: For list of minimum employees required by various business function unit. Once BCP has been initiated, each BCP Unit coordinator must ensure that the minimum employee requirement is met either by physically granting them workstation or providing Internet dongle to meet the operation requirement.

S.no.	Emergency Contact	Emergency No's
1	Delhi Police Department	100/112
2	Delhi Fire Department	101
3	Ambulance	108
4	Central Accident and Trauma Services	102/1099
6	Disaster Management & Mitigatio Unit, Nehru Place, New Delhi	+91-7947106659

- Process Dependency Records: For smooth operations function, BCP Unit coordinator must ensure that both upstream and downstream dependency of processes is working.
- RTO and RPO: IT Coordinator must ensure that their recovery systems adhere to these timelines.

- Resource/ Supplies Requirement: Each Administration/ Infrastructure coordinator must ensure that the minimum resource/supplies requirement is available at each site for any contingency.
- Critical Period: Critical Period outlines the urgency of Business hour.
- In case of exigency, the Admin Coordinator or any other BCP organization member must use this list to restore the vendor services.

26. Exercising and Validation Concept

26.1 Exercise objectives

To undertake a thorough and rigorous testing of the business recovery process, including the simulation of a disruptive event, which produces results which can be measured and evaluated together with feedback which enables the BCP to be enhanced and streamlined

26.2 Exercising scope

The tests will be carried out in a comprehensive and exhaustive manner so that all aspects of the plan are tested. The tests will be contributed by all business and support units within the organization.

26.3 Exercise schedule

A business continuity plan exercise/ test will be scheduled on a regular basis, by the BCP coordinator in conjunction with the BCP Team and business management teams. Exercises will be scheduled with consideration of factors such as seasonal production and business cycles.

26.4 Exercise methodology

A combination of tests and exercises will be conducted to validate both the business continuity plans and the alternate processing strategies that have been defined for the business process and clinical areas.

All the exercising methods shall be executed as and when required.

26.5 Announced and Unannounced Exercises

Announced exercises are scheduled exercises such as those involving actual resumption of computer processing at the alternate facility, during which production processing is usually not interrupted, but may be planned for actual resumption and validation. This type of test will not involve the entire business continuity organization, but will involve selected users (associated to the applications being recovered) along with computer operations and technical staff.

Unannounced exercises are surprise exercises that will involve only a small portion of the business continuity organization and few, if any, users. Call Notification and Tabletop are the types of exercises that can be unannounced since they would have the least impact/interruption on actual business functions. Unannounced exercises will be done at the discretion of business unit management.

26.6 Evaluation of Exercise

The results of all exercises will be evaluated by an unbiased validation team. This team will be made up of HUDCO, and are focused entirely on evaluating the continuing validity, currency and capability of the plan to resume HUDCO’s critical business processes in the event of a business disruption/disaster.

An exercise validation team holds the following responsibilities:

- Familiarization with the overall business continuity plan(s) in scope for the exercise.
- Understanding thoroughly the objectives of the exercise to be conducted.

- Monitoring and observing all the activities of the management teams and staff involved in the exercise.
- Ensuring that exercise objectives are met, from the IT and other stakeholder's points of view.
- Documenting findings related to the strengths and weaknesses observed during the exercise.
- Following up with the business process/plan owner to ascertain if changes required were completed.
- In addition to actions of the exercise validation team, each participant from the business process management/ staff will be asked to evaluate the effectiveness, success and value of the exercise.

26.7 Post-exercise reporting

The business process management/staff along with the test/exercise coordinator will document exercise results as soon as possible, but not later than three weeks after completion of an announced or unannounced exercise.

Selected members of the business unit management team will review the exercise results and identify actions necessary to resolve any gaps identified. The BCP coordinator will manage the review and coordinate appropriate changes/updates to the plan. The results of the review will be presented to the management team.

26.8 Change management process (in response to lessons learned)

Formal change management is implemented to cover any changes required to the BCP. This is necessary due to the level of complexity contained within the BCP.

27. Training and Awareness

Training and awareness programs prepare associates for their roles in the recovery process and continuously enhance the skills required to develop, implement, maintain, and execute BCM plans. These programs also create a state of readiness that will help protect the safety of the associates and of the business.

Awareness of the need for and the process of maintaining a viable continuity capability are essential. We at HUDCO will achieve it through formal education and training sessions that will be conducted on a needed basis. This is the way to provide the necessary awareness and understanding of the business continuity program and processes so that overall business continuity objectives along with the local business continuity plans are understood by personnel who are responsible for maintaining and executing the continuity/recovery processes.

HUDCO must define various mandatory & non-mandatory trainings for employees at all levels.

Objective

- Train key staff and management personnel who are required to maintain the plan in a constant state of readiness.
- Train the key staff and management personnel in their roles and responsibilities who are required to execute all/various plan segments and implement the alternate processing strategies to maintain critical business processing in the event of a disruption/outage or catastrophic disaster.

- Train key staff and management personnel on the communication process and responsibilities for those that will be affected by a business disruption/outage(s) and what is expected during an interruption to critical processing.
- Heighten planning awareness for staff not directly involved in maintaining and/or executing the plan.

28. Plan Maintenance Protocols

Board is responsible for approving HUDCO's Business Continuity Plan. ED(IT) has the authority to execute the Plan and for conducting its required annual review. The BCP will be modified more often on the occurrence of following situations:

- Major technology changes occur.
- The sensitivity of customer information increases.
- Internal or external threats to information change.

HUDCO will update this plan whenever there is a material change to HUDCO's operations, structure, business or location or to those of HUDCO's partners. In addition, HUDCO will review this Business Continuity Plan annually, to modify it for changes to operations, structure, business, or location.

HUDCO maintains copies of its BCP for inspection, along with the annual review and changes made to the Plan. An electronic copy of the Plan is located on the local as well as online HUDCO's document repository.

28.1 Teams and responsibilities

The BCP Head will remain in overall control of the BCP but other Coordinators will communicate their inputs on changes required in their own sections of the BCP. It is important that the relevant BCP Coordinators are kept fully informed regarding any approved changes to the plan.

28.2 Change control procedure for updating the plan

Formal change management is implemented to cover any changes required to the BCP. This is necessary due to the level of complexity contained within the BCP.

28.3 Maintenance schedule

Scheduled maintenance consists of update requirements that are based on the result of semi-annual structured walk-through and/or tactical exercises. The purpose of the semi-annual plan review is to determine whether changes are required to strategies, tasks/procedures, resource requirements, team assignments, notification and administrative issues pertaining to the business continuity plan(s).

The BCP Coordinator is responsible for initiating and coordinating scheduled maintenance activities.

29. Incidence Response Plan

29.1 Goals for Cyber Incident Response

When a cyber security incident occurs, timely and thorough action to manage the impact of the incident is a critical to an effective response process. The response should limit the potential for damage by ensuring that actions are well known and coordinated. Specifically, the response goals are:

1. Preserve and protect the confidentiality of constituent and employee information and ensure the integrity and availability of systems, networks and related data.
2. Help recover business processes after a computer or network security incident or other type of data breach.
3. Provide a consistent response strategy to system and network threats that put data and systems at risk.
4. Develop and activate a communications plan including initial reporting of the incident as well as ongoing communications, as necessary.
5. Coordinate efforts with external Computer Incident Response Teams and law enforcement.
6. Minimize organizations 's reputational risk.

29.2 Purpose and Scope

This document provides guidelines on responding to cyber security and data breach incidents in a consistent and effective manner. The plan establishes Incidence response to an incident with defined roles, responsibilities, and means of communication. Definition of incidence Impact and potential examples are given in Appendix – A.

29.3 Incident Response Life Cycle Process

Cyber incident response management is an on-going process with a cyclical pattern. The specific incident response process elements that comprise the Cyber Incident Response Plan include:

1. **Preparation:** The on-going process of maintaining and improving incident response capabilities and preventing incidents by ensuring that systems, networks, applications, and data handling processes are sufficiently secure, and employee awareness training is in place. Practice exercises (aka Table-top Exercises) for the IRT are conducted periodically, where various incident scenarios are presented to the Team in a practice session.
2. **Identification:** The process of confirming, characterizing, classifying, categorizing, scoping, and prioritizing suspected incidents.
3. **Notification:** Alerting IRT members to the occurrence of an incident and communicating throughout the incident.
4. **Containment:** Minimizing financial and/or reputational loss, theft of information, or service disruption. Initial communication with constituents and news media, as required.
5. **Eradication:** Eliminating the threat.
6. **Recovery:** Restoring computing services to a normal state of operation and the resumption of business activities quickly and securely. Provide reputational repair measures and news media updates, if needed. Provide credit monitoring services to effected constituents, or other remediation measures, as appropriate.
7. **Post-incident Activities:** Assessing the overall response effectiveness and identifying opportunities for improvement through, 'lessons learned' or mitigation of exploited weaknesses. Incorporation of incident's learnings into the cyber fortification efforts and the response plan, as appropriate.

8. These process elements are depicted in Figure 1, showing the closed loop nature of the process, in that the learnings from any prior incidents are used to improve the prevention and response process of potential future incidents.

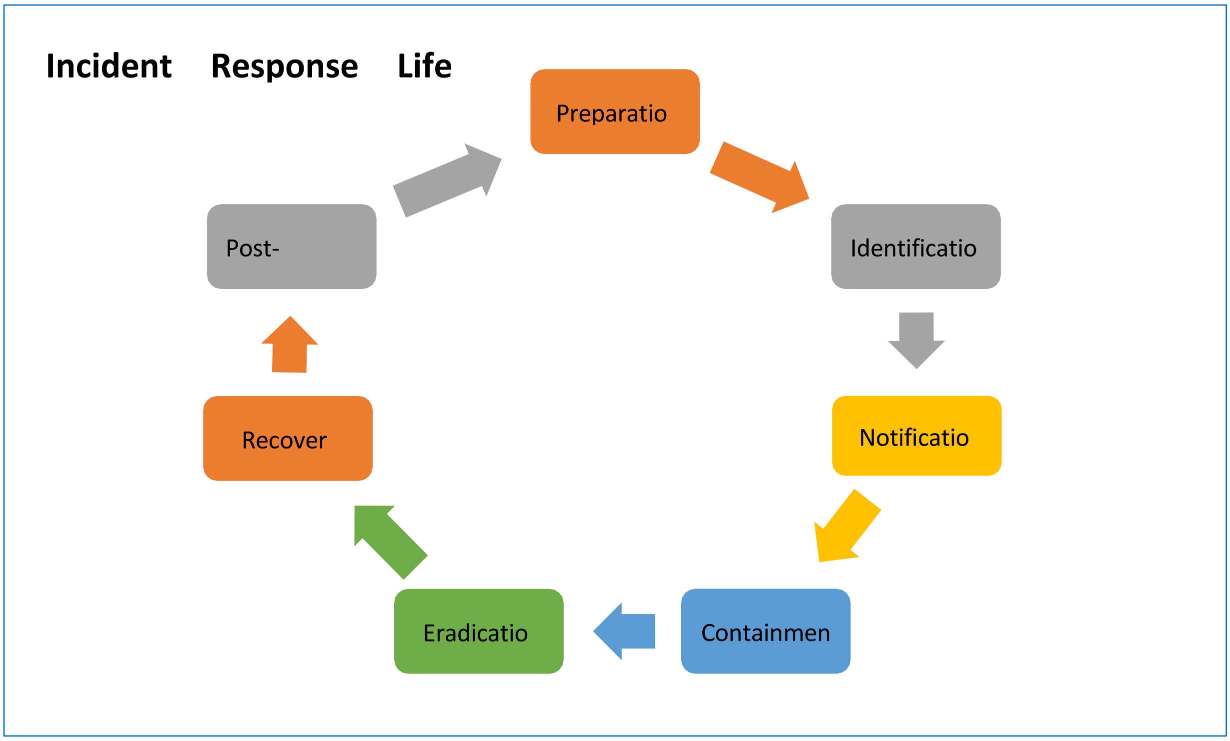


Figure 1

29.4 Incident Response Team (IRT)

A team comprised of company staff, advisors, and service providers shall be responsible for coordinating incident responses and known as the Incident Response Team (IRT). This team will have both primary members and secondary members. The primary members of the IRT will act as first responders or informed members to an incident that warrant IRT involvement, according to the incident's severity. The entire IRT would be informed and involved in the most severe incidents.

IRT members may take on additional roles during an incident, as needed. Contact information, including a primary and secondary email address, plus office and mobile telephone numbers shall be maintained and circulated to the team. The IRT will draw upon additional staff, consultants or other resources, (often referred to as Subject Matter Experts – SME's) as needed, for the analysis, remediation, and recovery processes of an incident. The Information Technology (IT) function plays a significant role in the technical details that may be involved in an incident detection and response and can be considered an SME in that regard.

29.5 Cyber Incident Response Team (IRT):

Primary Team Members:

Following Emergency Response Team was identified as per Office Order No. HUDCO/ITW/ERT/2023-24/01 or its amendments as required by HUDCO.

Sr. No.	Role	Name / Designation
1.	Chief Emergency Coordinator1	
2.	Chief Emergency Coordinator2	
3.	Network Coordinator/ Member Secretary	
4.	Software Coordinator	
5.	IT Security Coordinators	
6.	HR Coordinator	
7.	Administration Facilities	
8.	IT Infrastructure Coordinator	
9.	Emergency Response Staff	

Secondary Team Members:

Security event monitoring vendor and/or computer forensics vendor:

- SOC Admin | HUDCO Data Centre
- PR Department In-charge
- Cyber insurance provider – TATA AIG

29.6 Incident Response Process Detail

The detailed steps and general timing of an incident response are outlined below.

Process Phase & Approximate Timing	Process Detail Steps	Involved Parties
Identification (Hours)	1. Identify and confirm that the suspected or reported incident has happened and whether malicious activity is still underway. 2. Determine the type, impact, and severity of the incident by referring to 3. Take basic and prudent containment steps.	IT and SOC monitoring service provider
Notification (Hours – 1 Day)	1. Inform or activate the IRT, based on the severity of the incident, and provide the type, impact, and details of the incident to the extent that they are known. 2. Determine the need for Subject Matter Experts (SME) to be involved in the Containment, Eradication, and Recovery processes.	IT & IRT

Containment (Hours-2 Days)	1. Take immediate steps to curtail any on-going malicious activity or prevent repetition of past malicious activity. 2. Re-direct public facing websites, if needed. Provide initial public relations and other responses as required.	IRT, IT, SME's
Eradication (Days -Weeks)	1. Provide full technical resolution of threat and related malicious activity. 2. Address public relations, notification, and legal issues.	IT, IRT, SME's
Recovery (Weeks -Months)	1. Recover any business process disruptions and re-gain normal operations. 2. Address longer term public relations or legal issues, if required, and apply any constituent remedies.	SME's, IRT
Post-incident (Months)	1. Formalize documentation of incident and summarize learnings. 2. Apply learnings to future preparedness.	IRT

29.7 Preparation

- **System Inventory**: Maintain an updated inventory of critical systems, data, applications, and dependencies to ensure a clear understanding of assets that need protection.
- **Threat and Risk Identification**: Identify potential threats, vulnerabilities, and risks unique to the organization's operations, considering internal and external factors.
- **Preventive Measures**: Implement robust preventive measures such as firewalls, intrusion detection and prevention systems (IDS/IPS), secure access controls, and encryption to safeguard data and systems against unauthorized access and cyber threats.
- **Policies and Training**: Establish security policies and provide regular training to employees to enhance awareness and preparedness.
- **Regular Updates**: Ensure systems, software, and preventive tools are regularly updated and patched to address known vulnerabilities.

29.8 Incident Occurrence & Awareness

The way an incident becomes know will have an impact on the response process and its urgency. We become aware of an incident either though employees/SOC Team /technology providers/third-party informant.

29.9 Incident Response Tools

HUDCO should ensure the preparation of necessary tools and resources to effectively manage incidents. This includes:

- **Forensic Tools**: Equip teams with tools/service providers for investigating, collecting, and analysing data to identify the root cause of incidents.

- **Communication Systems**: Establish secure and reliable communication channels to ensure clear coordination during incident response and recovery.
- **Recovery Mechanisms**: Implement robust systems and processes to restore operations quickly and minimize disruptions, including backup solutions, disaster recovery plans, and system restoration tools.

29.10 Incident Identification

- Implement advanced monitoring tools and systems to detect anomalies and potential security breaches in real time.
- Establish a tiered classification system to assess the severity of incidents and prioritize response efforts based on their impact.
- Develop simple, clear, and accessible methods for staff and external stakeholders to report incidents promptly.
- Collaborate with law enforcement, regulatory bodies, and other relevant authorities to ensure compliance and effective incident handling.
- Prepare pre-approved templates and strategies for public statements to ensure timely, consistent, and accurate communication during an incident.
- Work closely with recognized cybersecurity agencies and law enforcement to address and mitigate threats effectively.
- Regularly update and refine these measures to stay aligned with emerging threats and compliance requirements.

29.11 Containment

- Identify and separate compromised systems to prevent the incident from spreading further within the network.
- Implement short-term measures to mitigate the immediate impact of the incident and stabilize operations.
- Collect, preserve, and document evidence following legal and forensic guidelines to ensure it is admissible in potential legal proceedings.
- Plan and implement permanent fixes that address the root cause of the incident, while minimizing disruptions to critical services and ensuring business continuity.

29.12 Eradication

This phase focuses on removing the root cause of the incident and ensuring that the systems are secure and stable. It involves:

- Analyse and determine the origin of the attack, including how it occurred and what systems were affected.
- Remove any malicious code, unauthorized software, or artifacts left by the attacker from the compromised systems.
- Address the vulnerabilities exploited during the attack by applying necessary updates, patches, or configuration changes to prevent recurrence.
- Conduct a thorough review to ensure that all affected systems and data have been restored to their secure and intended state, free from any lingering threats.

29.13 Recovery

- Rebuild or restore affected systems using clean, verified backups to ensure data integrity and eliminate any residual threats.
- Confirm that systems are operating securely and performing as expected before making them fully operational.
- Gradually bring systems back online in phases, allowing for careful monitoring of stability, performance, and security during each stage.
- Continuously assess restored systems to detect any lingering vulnerabilities or issues, ensuring a complete recovery.

29.14 Post-Incident Analysis

After an incident, conduct a thorough review to evaluate the nature and impact of the event, assess the effectiveness of the incident response process, and analyze team performance during the response. Document key insights, lessons learned, and any identified gaps to improve the Incident Response Plan (IRP) and strengthen future responses. Ensure compliance with regulatory requirements and internal policies by completing necessary reports and sharing findings with relevant stakeholders.

30 Type of incidents and Details of Agencies to be Informed

30.1 Incidents Reported to CERT-IN

HUDCO will report the cyber incident with in 6 hour of incident which may include out of applicable: -

- Targeted scanning/probing of critical networks/systems.
- Compromise of critical systems/information
- Unauthorized access of IT systems/data
- Defacement of website or intrusion into a website and unauthorized changes such as inserting malicious code, links to external websites etc.
- Malicious code attacks of reasonable severity such as spreading of virus/worm/Trojan/Bots/ Spyware/Ransomware.
- Attack on servers such as Database, Mail and DNS and network devices such as Routers vii. Identity Theft, spoofing and phishing attacks
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Attacks on Wireless networks
- Attacks on Application such as E-Governance, E-Commerce etc.
- Data Breach
- Data Leak
- Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers
- Attacks or incident affecting Digital Payment systems
- Attacks through Malicious mobile Apps
- Fake mobile Apps
- Unauthorized access to social media accounts
- Attacks or malicious/ suspicious activities affecting Cloud computing systems/servers/software/applications

- Attacks or malicious/suspicious activities affecting systems/ servers/ networks/ software/ applications related to Big Data, Block chain, virtual assets, virtual asset exchanges, custodian wallets, Robotics,
- Attacks or malicious/ suspicious activities affecting systems/ servers/software/ applications related to Artificial Intelligence and Machine Learning

Following are the contact details of related agencies:

1) CERT-In:

Cyber Security Incidents to be reported to CERT-In

Website: https://www.cert-in.org.in

Email: incident@cert-in.org.in

Contact No:011-24368551

2) Indian Cybercrime Coordination Centre (I4C)

For Reporting Cyber Fraud & Crime, report to IHC, established by MHA

website: https://www.cybercrime.gov.in

Call: 1930

Following incidences to be informed based on their level of severity:

Incident Type	Type Description	Severity Level (5: Most severe)	Incidence Response
Denial of Service (DoS), Distributed DoS (DDOS), Ransomware attack, Intrusion	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources.	5	Remediation coordinated by IT Department, related members of IRT, Both Primary and secondary team SMEs. For further Forensics, and Possible Legal Counsel, Report to CERT-In and I4C Legal Counsel notified if a PII breach
Data Breach/ Data Leak	Internal Data Breach/ Leak or ERP Data	4	
Unauthorized Access	When an individual or entity gains logical or physical access without permission to a company network, system, application, data, or other resource.	4	

Website Cyber Incidence	Defacement of website or intrusion into a website and unauthorized changes such as inserting malicious code, links to external websites	4	
Suspected PII Breach	1.An incident where it is suspected that Personally Identifiable Information (PII) has been accessed 2.involves a suspected loss of sensitive information (not PII) that occurred because of Unauthorized Access, Malicious Code, or Improper/Inappropriate use	3	
Phishing E-mail attack	Data Compromise through E-mail Phishing attack	3	To be handled by E-mail Security Solution
Malicious Code	Malicious software (e.g., a virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.	2	Remediation coordinated by IT and SME, to be reported to related members of IRT for necessary action
Affects data or services of a single individual/group of individuals with no sensitive data	Compromised computers with virus etc. with no sensitive data	1	focus is on correction and future prevention
Occurrences of very minor or undetermined focus, origin and/or effect	Impaired computer requiring review of system access logs, AV scans, or other repairs.	0	Hardware Team to be informed by secondary team

30.2 Information Recording

Information recording is very important during an incident, not only for effective containment and eradication efforts, but also for post-incident lessons learned, as well as any legal action that may ensue against the perpetrators. Each member of the IRT shall be responsible for recording information and chronological references about their actions and findings during an incident, using the IRT Incident Record Form in Appendix B.

Appendix-A

Incident Impact Definitions

Security Objective	General Description	Potential Impact Examples		
		Low	Medium	High
Confidentiality: Preserving restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have the following adverse effect on organizational operations, organizational assets, or individuals.	Limited to a single or several Users or computers in an isolated fashion, with easy remediation	Involving or affecting a group of Users, resulting in access to proprietary information. Limited or no external exposure.	A severe breach of proprietary information with external exposure.
Integrity: Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have the following adverse effect on organizational operations, organizational assets, or individuals.	Inadvertent or non-malicious alteration or deletion of company data that is easily remediated.	An on-going improper data alteration act (or series of acts) of malicious or negligent nature that will having a moderate business impact.	A massive alteration or destruction of company data of a malicious or obstructive nature.
Availability: Ensuring timely and reliable access to and use of information systems.	The disruption of access to or use of information or an information system could be expected to have the following adverse effect on organizational operations, organizational assets, or individuals.	Isolated outage or inaccessibility affecting a limited number of Users for a short amount of time (< 2 hours)	A widespread outage or inaccessibility of a primary business system lasting more than 2 hours, but less than a day	Severe outage or inaccessibility of the company business systems lasting a day or more.

Appendix-B

IRT Incident Record Form

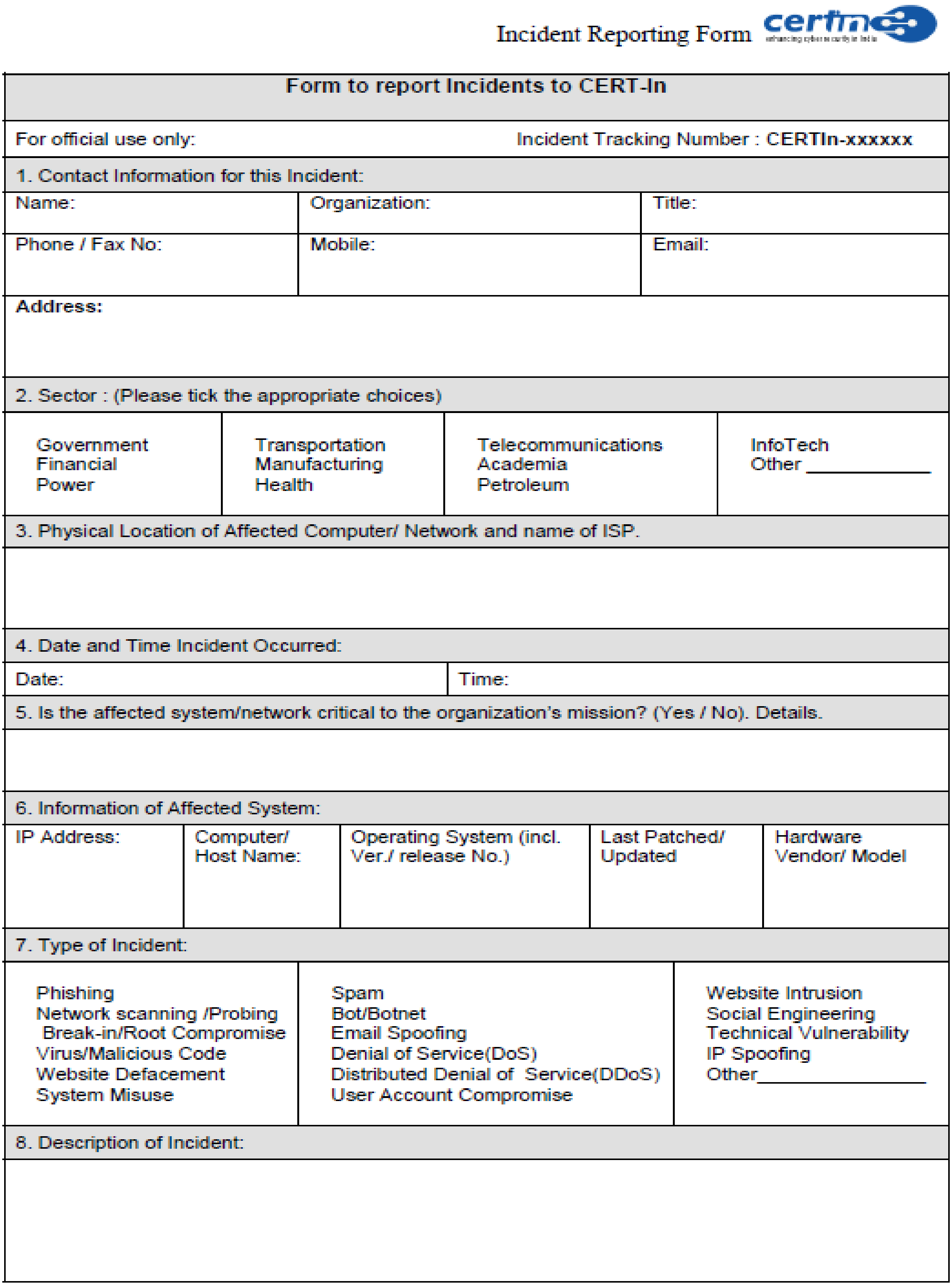
Date/Time	Detail

lincident____

Discovery Date: ___________________

Recorded By: ____ Page _________of ________ Pages

CERT-In Incident Report Form



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.

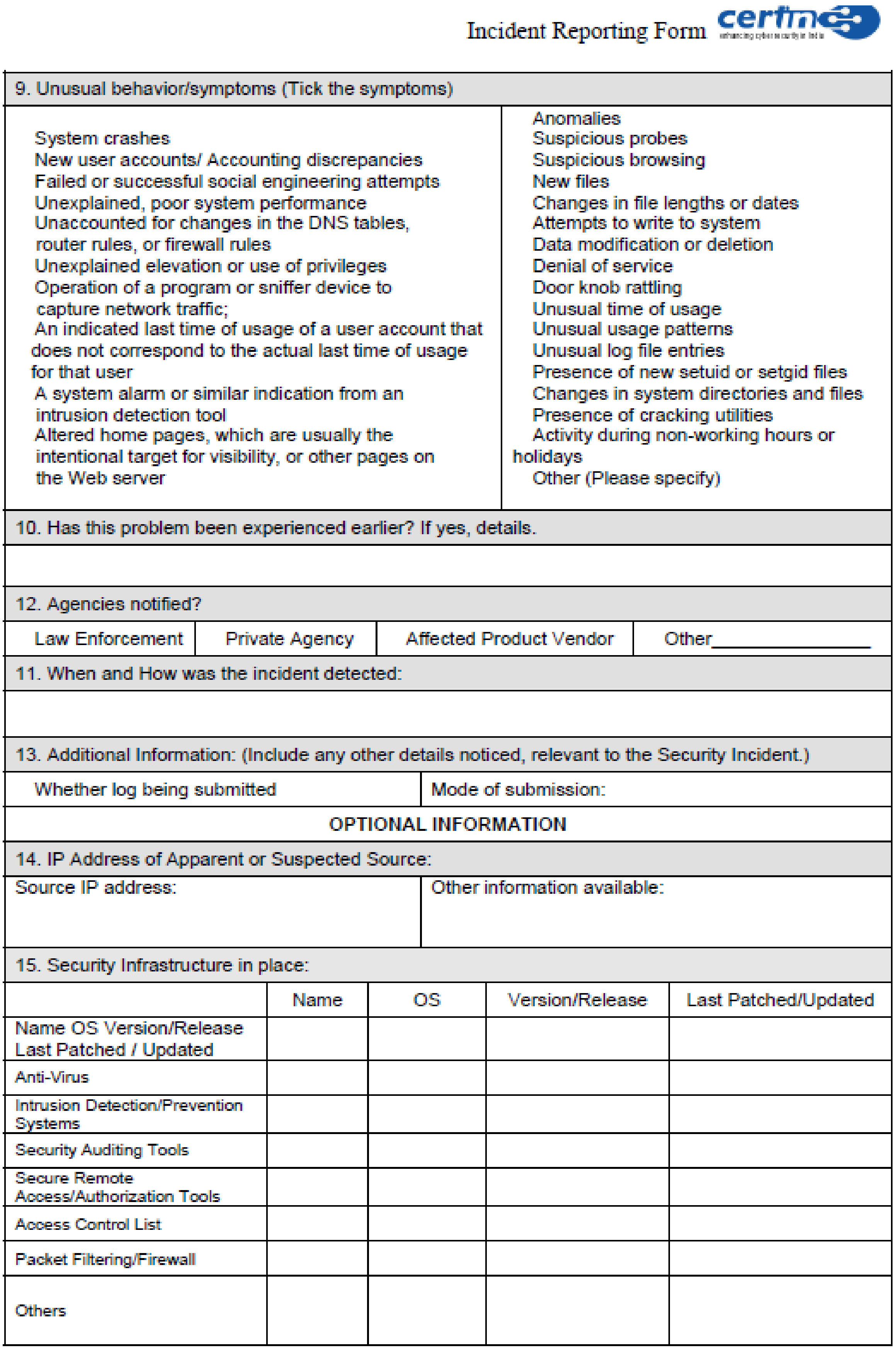
6. Information of Affected System:

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:

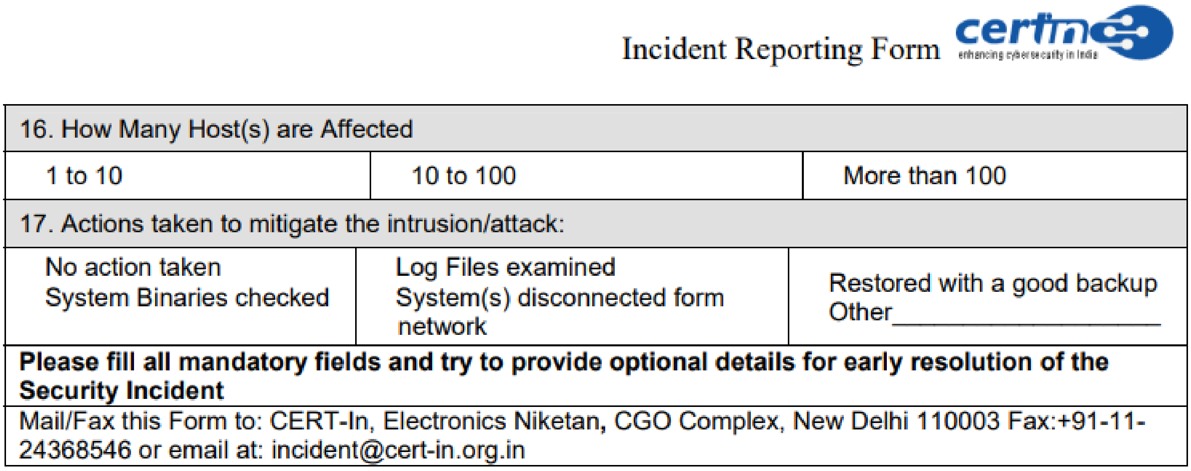
OPTIONAL INFORMATION

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		

Appendix-C

AIIMS Cyber Incidence Use Case

Incident - Ransomware Attack AIIMS Servers.

Impacts of the attack:

All the following online services are disrupted for 19 days

- Smart Billing
- Report generation
- Appointment bookings
- Patient out billing
- Patient registration

How the attack occurs:

- AIIMS has the total 40 Physicals Servers and 100 Virtual servers are present and hosted by NIC
- Out of all these, Five Servers were Compromised by the attackers. Many systems were encrypted by ransomware. Many patients' sensitive data along with VIPs data, former prime minister health reports were also in the hands of attackers.

How AIIMS handled the situation (Containment)-

On 23rd November 2022 Morning the systems of AIIMS were became very slow and after sometime all the systems were acts abnormally and online services are disrupted AIIMS Technical team Approached NIC and Cert-in they began to investigate the scenario and found out that all the files' extensions are changed to unknown format that signs the ransomware attacks was confirmed by the agencies All the effected Systems were isolated and all the devices were removed from the network. The investigation agencies like cyber forensics, Delhi cyber police and third-party companies were helped to AIIMS in neutralizing the impact Delhi police has filed a FIR Under section 66F IT ACT Cyber terrorism and extortion. After the Investigation done by Cert –IN and NIC and other agencies together and found that AIIMS uses one software for email service called as Zimbra, in this software due to outdated version, the attackers were able to inject malicious ransomware file and got executed.

Resolution– Techs isolated the effected systems removed from network and they sanitized the whole network and updated the Zimbra email service version then they again re-hosted in new servers.

Finally on December 12th all the E-services was restored and functioning properly.