BMD SECURITIES LIMITED

STANDARD OPERATING PROCEDURE

Policy created by	Compliance Team
Policy reviewed by	Designated Officer
Policy reviewed on	31-12-2024
Policy Approved by	Board of Directors
Policy approved on	28-04-2025

Version – 1.2

Cyber Security incident handling process document

Cyber security incident management is not a linear process; it's a cycle that consists of a preparation phase, an incident detection phase and a phase of incident containment, mitigation and recovery. The final phase consists of drawing lessons from the incident in order to improve the process and prepare for future incidents.

Drawing up a cyber security incident response plan is an important first step of cyber security incident management. It is also crucial that management validates this plan and is involved in every step of the cyber security incident management cycle.

The following elements should be included in the cyber security incident response plan

Identification of the assets that need to be protected:

- ✓ Identification and assignment of responsibilities in the context of a cyber-security incident;
- ✓ In house capabilities or contracts with external experts for incident response and/or forensic investigation in case of an actual cyber security incident;
- ✓ The equipment and technology to detect and address a cyber-security incident;
- ✓ A basic containment strategy:
  - Disconnect the systems immediately in order to recover as quickly as possible?
  - Or take the time to collect evidence against the cybercriminal who perpetrated the system?
- ✓ A communication strategy for management and for authorities such as Depository and SEBI.

A good cyber security incident response plan can make the difference between a cyber-security incident and a cyber-security crisis. The pace at which we able to recognize, analyses and respond to an incident will influence the damage done and the cost of recovery. Such a cyber-security incident response plan should not be limited to technology. Processes, people and other aspects of organization are also important elements to take into consideration.

Important terms to be known for Cyber Security incident handling

- ✓ **Cyber Security Event** - A cyber security change that may have an impact on our operations (including mission, capabilities, or reputation).
- ✓ **Cyber Security Incident** - A single or a series of unwanted or unexpected cyber security events that are likely to compromise our operations.
- ✓ **Cyber Security Incident Management** - Processes for preparing, for detecting, reporting, assessing, responding to, dealing with and learning from cyber security incidents.

Basic Principles for examine the cyber security incidents

- ✓ **There is no simple one-size-fits-all solution** -When it comes to Cyber Security there is no one-size-fits-all solution. What will work for us will depend on its mission and goals, the kind of infrastructure and information we are protecting, available resources, etc. Finally, recognise that some techniques will only be learned with time and experience.

- ✓ **Top management's commitment** - Cyber security incidents are a risk that should be incorporated in the overall risk management policy of company. Furthermore, managing cyber security incidents does not just mean applying technology. It also requires the development of a plan that is integrated into the existing processes and structures, so that it enables rather than hinders critical business functions. Therefore, top management should be actively involved in defining a cyber security prevention and incident response plan, because top management's explicit support through appropriate internal communication and the allocation of personnel and financial resources is key to the success of the plan. The Designated Officer will be aware both of the risks of cybercrime and of his own exemplary role in encouraging all employees of company to assume their responsibility.
- ✓ **Involve every employee of the Company** - It is often said that humans are the weakest link when it comes to cyber security. Having said that, it is also important to realise that the employee of company have great potential to help detect and identify cyber security incidents. Make sure that every employee of our company is aware of the cyber security incident response plan and of their own role within it; even if this just means informing the right person.
- ✓ **Keep an offline copy of the documents need during an incident**–We have to keep in mind that when a cyber-security incident occurs, we may not always have access to the files on our computer. It is always a good idea to keep a hard copy/offline copy of any document we are likely to need during a cyber-security incident or crisis.
- ✓ **Don't link backups to the rest of the system** - When it comes to backups, it is not only crucial to have them. It is also very important to have a backup that is not linked in any way to the rest of the system. If the backup is linked to the system, chances are that the infection of the system also spreads to the backup, which makes the backup useless.
- ✓ **The importance of logging and keeping those logs during a certain time (up to 6 months)** - Logs can help to trace back the origin of the cyber security incident. This is not only important to be able to identify the cybercriminal; it will also help the companyto get back to business as soon as possible.
- ✓ **Ensure to take all legal aspects into account when managing a cyber-security incident** -Evidence will only be admissible in Police or cyber security cell if it has been collected in respect of all applicable laws and regulations.
- ✓ **Document every step of a cyber-security incident**–Ensure to note down any action that is taken, such as the reporting of the incident, the collecting of evidence, conversations with users, system owners and others, etc. When something goes wrong it may allow looking back and evaluating where and why the problem started. Furthermore, documenting the cyber security incident response will ensure that the knowledge regarding what is going on is not just in a few people's heads.

Cyber Security Action / Response Mechanism

- ✓ **IDENTIFY THE ASSETS AND POTENTIAL THREATS–**
  - When hit by an incident the first questions that will arise are: which assets are at risk?
  - And which of those assets are vital for the business's activity?

We will have to decide which assets need attention first in order to remain in business and keep the damage to business as low as possible. That's why it is crucial to identify, document and categorise 'vitals': the assets of company depend on to conduct its core activities. This will help to identify where to apply which protective measures and to take quick and justified decisions during the incident management process. The following will give an idea of what those 'vitals' could be: management, company, processes, knowledge (e.g. intellectual property has been stolen), people, information (e.g. data sets have been stolen or altered), and applications (e.g. website is down or defaced, infrastructure (e.g. system and/ or network connections are down), financial capital (e.g. bank accounts). It's also a good idea to identify vulnerabilities and potential threats.

✓ HOW TO IDENTIFY, DOCUMENT AND CATEGORISE VITALS, VULNERABILITIES AND POTENTIAL THREATS?

- **Identify the business and the resources that need to be protected**
  - ❖ Determine which are core business activities that enable our companyto exist, to achieve its corporate objectives and generate income.
  - ❖ For each of those activities, identify which IT systems (databases, applications, control systems) and network connections are supporting them.
  - ❖ Determine also where these IT systems are located: on own servers or in the cloud
  - ❖ When identifying these assets, don't forget flows of information to third parties (suppliers, clients, etc.).
- **Determine what the crown jewels are**
  - ❖ Determine now which assets, data, processes or network connections are so important for our company that we lose (control of) them, we will bein big trouble or even out of business?
- **Assign business priorities for recovery**
  - ❖ This priority will determine the order in which the systems will be re-established. In most cases the underlying network will need the highest priority, as this is not only the path for system administrators to reach the assets but also the path that cyber criminals use to attack the systems. As long as criminals can use the network connections, any other recovery activity might be undone by them. When assets have equal priorities, parallel recovery activities might be considered.
- **Document how the systems work and keep this documentation up to date**
  - ❖ Ensure that the way systems work is documented and that this information is kept up to date and available on the incident response team's documentation systems.

Especially needed documents are:

➢ **Network Scheme** displaying the network architecture with internal network segmentation and the different gateways to external networks, DMZ, VPN, IP-address ranges used. This scheme should also include the different security devices in place that might contain logging information of network activity (firewalls, (reverse) proxy servers, intrusion detection systems, security incident event management systems). For larger companies with complex networks, it is also necessary to have a high-level version of the network architecture so that one can quickly get an idea of the network in case of emergency.

- **Equipment and services inventory.** This inventory will include, for the vital assets in the environment, all the different servers and the network components used for delivering the different corporate services. As some of these (physical) servers might be servicing multiple business functions it is important to know per server which services are running on them.
- **Account and access lists.** At all times it is important to know who has the right to access, use and or manage the network and the different systems in it. This will allow to detect any strange or abused accounts during an incident

✓ ASSIGNING RESPONSIBILITIES AND CREATING A CYBER SECURITY INCIDENT RESPONSE TEAM–

It is important that the roles and responsibilities in case of a cyber-security incident are documented in the cyber security incident response plan.

When drafting the description of these roles and responsibilities, we should ask the following questions:

- Who is the internal contact point for cyber security incidents? And how can he be contacted?
- What are the different incident response tasks? And who is responsible for doing what?
- Who is managing the incident from business/technical side? This should be someone within the company with decision-making authority, who will follow the incident from the beginning until the end.
- Who will communicate with senior management?
- Who can engage the external incident response partner?
- Who can file a complaint with law enforcement/inform the regulatory bodies?

In order to adequately address a cyber-security incident, different skills are needed to take up the different responsibilities and necessary roles of an efficient incident response.

SKILLS	RESPONSIBILITIES	ROLES
Incident management	Manage the cyber security incident from the moment of its detection until its closure.	Cyber security Incident response manager – Designated Officer
Business decision capability	Assessing the business impact and act upon it. Engage the right resources. Take decisions on how to proceed e.g. decide if the internet connection of a compromised system can be shut down and when is the most appropriate time. Decide when to start clean-up activities. Decide whether to file a complaint or not.	Management
Network management capabilities	Technical know-how on network (firewall, proxies, IPS, routers, switches). Analyse, block or restrict the data flow in and out of the network. IT operations Information security and business continuity	IT technical support staff

Workstation and server administrator capabilities (admin rights)	Analyse and manage compromised workstations and servers.	IT technical support staff
Legal advice	Assess the contractual and judicial impact of an incident .Guarantee that incident response activities stay within legal, regulatory and our boundaries. Filing a complaint.	Designated Officer
Communication skills	Communicate in an appropriate way to all concerned stakeholder groups and answer clients immediately	Designated Officer
Physical security	Handle the aspects of the incident that are linked to • the physical access to the premises • The physical protection of the cyber infrastructure.	IT technical support staff

- ✓ **CYBER INCIDENT RESPONSE TEAM-** In an ideal world, every companyshould have an incident response team that is convened whenever there is an incident. Of course, the size of the company determines the size and the structure of the incident response team. Smaller companies that do not have the resources for an actual team could designate a first responder – ideally someone with business decision capability – amongst their personnel. In case of a cyber-security incident, he or she should contact external help, but remains the person ultimately responsible for the incident response within the company. The composition of this incident response team will be determined by the different skills that are needed to handle an incident. For smaller companies, some of these skills may have to be found outside the company and contacted by the first responder.

- ✓ **HARDWARE AND SOFTWARE FOR CYBER SECURITY INCIDENT MANAGEMENT -**To improve the maturity and efficiency of the incident response team, the appropriate tools need to be in place. It is important that the incident response team disposes of autonomous systems and tools that permit them to take care of an incident even if the corporate network has been compromised. This means that when thesystems or networks are no longer available, the system of the incident response team still is. Incident procedures and contact lists have to be available on these systems.

CLASSIFICATION OF INCIDENTS ON THE PARAMETERS OF RISK CATEGORIES:

- ✓ Cyber security incident response has become an important component of information technology (IT) programs. Cyber security-related attacks have become not only more numerous and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.

- ✓ The incident response process has several phases. The initial phase involves establishing and training an incident response team, and acquiring the necessary tools and resources. During preparation, we also attempt to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk

assessments. However, residual risk will inevitably persist after controls are implemented. Detection of security breaches is thus necessary to alert us whenever incidents occur. In keeping with the severity of the incident, we can mitigate the impact of the incident by containing it and ultimately recovering from it. During this phase, activity often cycles back to detection and analysis—for example, to see if additional hosts areinfected by malware while eradicating a malware incident. After the incident is adequately handled, we issue a report that details the cause and cost of the incident and the steps should take to prevent future incidents

- ✓ Periodic risk assessments of systems and applications should determine what risks are posed by combinations of threats and vulnerabilities. This should include understanding the applicable threats, including organization-specific threats. Each risk should be prioritized, and the risks can be mitigated, transferred, or accepted until a reasonable overall level of risk is reached. Another benefit of conducting risk assessments regularly is that critical resources are identified, allowing staff to emphasize monitoring and response activities for those resources.

- ✓ Weshall carry out risk assessment to examine the incident and classify them into High / Medium / Low risk as per the cyber security handling document and should take necessary action to minimize the loss and destruction and to prevent the company from such threats and vulnerabilities.

REPORTING OF INCIDENT TO CERT – IN

We should always seriously consider reporting cyber-security incidents to the Indian Computer Emergency Response Team, CERT-IN. Reporting to the CERT-IN is vital in determining whether the incident is isolated or not and allows to keep track of threat trends in India. The CERT-IN will be able to provide some information and advice related to the incident that can help the victim to take effective countermeasures. Furthermore, the information provides may help to prevent attacks on other computer systems.

The following information should be reported:

- ✓ Contact details
- ✓ The type of the incident
- ✓ The date of the incident
- ✓ Is the incident ongoing?
- ✓ How did company notice this incident?
- ✓ What's the impact of the incident?
- ✓ Have company already taken actions or measures? If so, which ones?
- ✓ Does company have logs or other useful data?
- ✓ Who have company already informed?
- ✓ What company expecting from the report?

We shall submit the overall details of the incident to Depository and SEBI whether the same has been reported or not reported to CERT-IN. Furthermore, if the incident is not reported to CERT-IN, members shall submit the reasons for the same to the Depository and SEBI.

FILING A COMPLAINT WITH LAW ENFORCEMENT AGENCIES

Communication to law enforcement authorities must be made as soon as possible after discovery of the cyber security incident, given the volatility of traces and actions that need to be taken (Internet identification, etc.). For prosecution to be successful, the chain of custody needs to be preserved in a legally accepted manner, which requires the evidence to be preserved immediately after the detection of the incident.

Judicial authorities need to possess the available information regarding the incident in order to make a qualification of the offence and proceed with the identification of the suspect. The information that should be communicated to the police in case of Internet fraud (a 'traditional' crime committed by electronic means) may not be entirely the same as the information the police needs in case of IT crime (hacking, sabotage, espionage). In the course of the investigation, additional information will be requested, collected and searched for by the investigators. It is of the outmost importance that the services provide the assistance and input requested by law enforcement, to help advance the investigation.

- ✓ **POLICE:** If our company is impacted by an incident and as such has been the victim of an offence; we can decide to lodge a complaint. By default, we should go to the local police station or the police station of choice. For more complex cases, the local police will get support from the CERT-IN / MHA / Cybercrime police, specialised in dealing with IT crime (hacking, sabotage, espionage). If the case concerns a critical infrastructure or a sector with specific rules, a special procedure may apply.

- ✓ **CYBER SECURITY CELL**: It is also possible to file a complaint directly with a Cyber security cell. This should be an exceptional measure. Furthermore, we will probably have to advance the costs of the investigation, because the Cyber security cell is conducting it at specific demand.

- ✓ **INFORMATION TO DEPOSITORY AND SEBI**: We shall submit details on whether the incident has been registered as a complaint with law enforcement agencies such as Police or cyber security cell. If yes, details need to be provided to Depository and SEBI. If not, reason for not registering complaint should also be provided to Depository and SEBI.

- ✓ **INFORMATION TO DOS-MIRSD and CISO OF SEBI**: The details of reported incidents and submission to various agencies by we shall also be submitted to Division Chiefs (in charge of divisions at the time of submission) of DOS-MIRSD and CISO of SEBI.

Quarterly Reporting of Cyber Incidents

The Designated Officer of our company(appointed in terms of para 6 of the SEBI Circular dated December 03, 2018) shall continue to report any unusual activities and events within 24 hours of receipt of such Information as well as submit the quarterly report on the cyber-attacks & threats within 15 days after the end of the respective quarter to the respective depositories and exchanges.

Most Common Incident types and how to neutralize them

INCIDENT TYPE	DEFINITION	POSSIBLE TARGET	VULNERABILITIES THAT MIGHT BE EXPLOITED	POSSIBLE REACTIONS
Social Engineering: (Spear) phishing, vishing (phone phishing)	Manipulating and tricking someone into revealing information that (e.g., password for financial information) that can be used to attack systems or networks	Management	As deems fit.	As deems fit.
(spear) phishing, vishing (phone phishing)	Attempt to acquire sensitive information (e.g. customer logins & passwords) from customers by impersonating a legitimate and trusted person or XYZ Company.	Management	As deems fit.	As deems fit.
Unauthorised access	When a person gains logical or physical access without permissionto a network, system, application, data, or other IT resource.	Customer information Credit card information Applications creating or processing payments Websites and services	Passwordcracked orsniffedUnpatched system vulnerabilities Social engineering Careless users or weak procedures	Patch vulnerabilities or block exploitation Check for malware (rootkits, backdoors, Trojans) Change passwords or inactivate accounts Forensic evidence gathering Block (network) access to the targeted resources
Denial of service	Any attack that prevents or impairs the authorised use of networks, systems or applications byexhausting resources.	Mail system Network appliances Application servers Web sites and services	Spam filter weaknesses Unpatched system vulnerabilities Weak configuration of systems or appliances	Block traffic Contact ISP Disconnect infected system(s)
Malicious code attack	A malicious code attack is any (large- scale) infection or threat of infection by a virus, worm, Trojan horse, or other code-based malicious entity	Any server or even appliance in the network could be the target of a malicious code attack,but some systems have a higher risk profile(e.g.	Unpatched system vulnerabilities (e.g. Flash or JavaScript) Anti-virus not installed, not active or signature file not up to dateInappropriate or imprudent user behaviour (e.g. using infected USB memory device)	Block malicious web traffic Apply patches Update anti-virus signature files. Run virus clean-up tool if available. Run vulnerability assessment tool to list vulnerable resources

		systems directly or indirectly connected to the outside world). Any end user workstations could be targeted via e-mail, USB storage devices, visits to web sites and web applications, etc.		Completely reinstall infected system Shut down vulnerable services Shut down or disconnect infect system(s)
Inappropriate usage	An inappropriate usage incident is any incident involving an internal employee or contractor violating a code of conduct or a computer policy. Inappropriate behaviour is not always malicious and targeted. Sometimes a user will simply act carelesslyor even be completely unaware of the standard operating procedure or code of conducthe / she has infringed. The inappropriate behaviour will sometimes constitute a serious security incident in itself, but it can also be the cause or trigger ofa serious incident (like malware infection, loss of critical data)	Payment transactions Credit card information Customer commercial and personal information Confidential information in general	Weak management or control of confidential data Bad user password management Lack of segregation of duties, accumulation of access rights Lack of application security or monitoring Lack of procedures or control to enforce policies and codes of conduct	Inform and get advice from Compliance and/or the legal department Inactivate users or withdraw access rights Make forensic copies of logs and other crucial information to trace and prove what happened Check logs and other information for traces of the infringement
Fraud	Fraud is a kind of inappropriate behaviour that is inherently malicious in nature, and aimed at personal enrichment by abusing company systems, applications or information.	Management	As deems fit.	As deems fit.
Data loss or theft	This is an incident that involves the loss or theft of confidential information. Information can be	Personal information about employees or	Personal information about employees or customers (protected by privacy laws or	Assess the level of protection of the data, if any (encryption,

	confidential because of the value it has for the company, or because it is protected by internal or external regulations. Data loss incidents can have a big financial impact, due to possible financial liability or damage done to the company image, should the information itself or the fact that is has been lost become public or known to the wrong people.	customers (protected by privacy laws or concerns) Credit card information Customer commercial information Confidential balance sheet information Confidential information about company strategy, on-going projects and decisions, etc	concerns) Credit card information Customer commercial information Confidential balance sheet information Confidential information about company strategy, on-going projects and decisions, etc.	password protection, specific device required to read the data) Inform and get advice from Compliance and/or the legal department or from the external legal adviser Inform Communications department and management, define a communication strategy Inform the owner of the lost or stolen data
Brand abuse	This is an incident where someone is abusing the brand and registered trademarks.	Registration of DNS names containing the brand Spoofing of website designs Spoofing of e-mail addresses and e-mail templates	Not applicable	Inform police (in case of theft) Request a takedown of the website Inform customers about the existence of this

Change in the Standard Operating Procedure will be adopted as and when required by the company and is binding on all the Staff/Employees/and Directors of the Company.

BMD Securities Limited

Utpal Mallick

CISO

Dated: - 30-04-2025