Incident Management Policy

Document Summary

Item	Value
Organization	
Document Name	Incident Management Policy
Classification	Public
Compliance Reference To:	

Document Revision History

Date	Version	Prepared By
16th April 2016	1.0	Gaurav Amar

Document Review History

Reviewed By	Version	Date	Signature

Reviewed Vajallyog 29/1/17

Policy Controls

1. Purpose of the Incident Response Plan

An Incident Response Plan is required in order to bring needed resources together in an organized manner to deal with an adverse event related to the safety and security of Organization's Business & Information Assets. This adverse event may be malicious code attack, unauthorized access to Organizational systems, unauthorized utilization of Organization services in denial of service attacks, general misuse of systems, or hoaxes.

2. Purpose of the Incident Response Team

The purpose of Incident Response Team is to:

- Protect Organizational Information assets,
- Provide a central organization to handle incidents
- Comply with (government or other) regulations,
- Prevent the use of Organizational system in attacks against other systems (which could cause us to incur legal liability).
- Minimize the potential for negative exposure.

3. Incident Classification

Security incidents will be classified according to incident categories and severity of incident. Incident response will be based on classification.

A. *Incident Categories*

The following categories will be used to describe IT security incidents at PVR Ltd. A single incident may have several different categories.

1. Confidential data exposure
    - Customer Account details
    - Credit Card information
    - Identity theft
    - Other
2. Criminal activity/investigation
    - Search warrant or other court order
    - Litigation hold request (ala e-Discovery)
    - Online theft, fraud
    - Threatening communication

- Pornography
- Physical theft, break-in

3. Denial of Service
   - Single or distributed (DoS or DDoS)
   - Inbound or outbound
4. Malicious code activity
   - Worm, virus, Trojan
   - Botnet
   - Key logger
   - Rootkit
5. Policy violation
   - The Organization's policy violation
   - Violation of student code of conduct
   - Personnel action/investigation
6. Reconnaissance activity
   - Port scanning
   - Other vulnerability scanning
   - Unauthorized monitoring
7. Rogue server or service
   - Rogue file/FTP server for music, movies, pirated software, etc.
   - Phishing scam web server
   - Botnet controller
8. Spam source
   - Spam relay
   - Spam host
   - Computer on a block list
9. Spear Phishing
   - Scam e-mail targeting a relatively large number of <Name of the Organization> e-mail addresses
10. Unauthorized access
    - Abuse of access privileges
    - Unauthorized access to data
    - Unauthorized login attempts
    - Brute force password cracking attempts
    - Stolen password(s)
11. Un-patched vulnerability
    - Vulnerable operating system
    - Vulnerable application
    - Vulnerable web site/service
    - Weak or no password on an account
12. Web defacement
    - Defacement of web site
    - Inappropriate post to Bank's comments/blog section
    - Redirected web site

13. Un-authorized network access
    - Wire-less
    - Rogue LAN connection
    - Wire-tapping
14. No Incident or False-positive
    - When investigation of suspicious activity finds no evidence of a security incident

B. *Incident Severity*

An incident will be categorized as one of three severity levels. These severity levels are based on the impact to the organization and can be expressed in terms of financial impact, impact to manufacturing, impact to sales, impact to company's image or impact to trust by company customers, etc. Following table provides a listing of the severity levels and a definition/description of each severity level.

Severity Level	Description
Low	Incident where the impact is minimal. Examples are harmless email SPAM, isolated Virus infections, etc.
Medium	Incident where the impact is significant. Examples are a delayed ability to order or manufacture [Product Name], delayed delivery of critical electronic mail or EDI transfers, etc.
High	Incident where the impact is severe. Examples are a disruption to the manufacturing or sales processes, company's proprietary of confidential information has been compromised, a virus or worm has become wide spread and is affecting over 30 percent of the employees, or Executive management has reported it.

4. Responding To An Incident

Six stages of response are described below:

4.1 Preparation

One of the most important facilities to a response plan is to know-how to use it once it is in place. Knowing how to respond to an incident BEFORE it occurs can save valuable time and effort in the long run.

4.2 Identification

Identify whether or not an incident has occurred. If one has occurred, the response team can take the appropriate actions. The approach to the Identification Stage involves:

1) Validating the incident
2) If an incident has occurred, identify its nature
3) Identifying and protecting the evidence
4) Logging and reporting the event or incident.

When a staff member notices a suspicious anomaly in data, a system, or the network, he or she begins this identification process or immediately notify the concerned person(s).

4.3 Containment

It involves in limiting the scope and magnitude of an incident. Because so many incidents observed currently involve malicious code, incidents can spread rapidly. This can cause massive destruction and loss of information. As soon as an incident is recognized, immediately begin working on containment. A decision on the operational status of the compromised system itself will be made. Whether this system should be:

1) Shut down entirely
2) Disconnected from the network or
3) Be allowed to continue to run in its normal operational status (so that any activity on the system can be monitored) will depend on the risk to assets threatened by the incident.

4.4 Eradication

Removing the cause of the incident can be a difficult process. It can involve virus removal, conviction of perpetrators, or dismissing employees. Should follow good practices:

1) ***Determine the Cause and Symptoms***
   Use information gathered during the containment phase and collect additional information. If a single attack method cannot be determined list and rank the possibilities.

2) ***Improve Defenses***
   Implement appropriate protection techniques such as firewalls and/or router filters, moving the system to a new name/IP address, or in extreme cases, porting the machine's functions to a more secure operating system.
3) ***Perform Vulnerability Analysis***
   Use of vulnerability analysis tool to scan for vulnerable systems that are connected to affected systems.

4.5 Recovery and Closure

Restoring a system to its normal business status is essential. Information Security Office reviews the tracking system and closes tickets when appropriate.

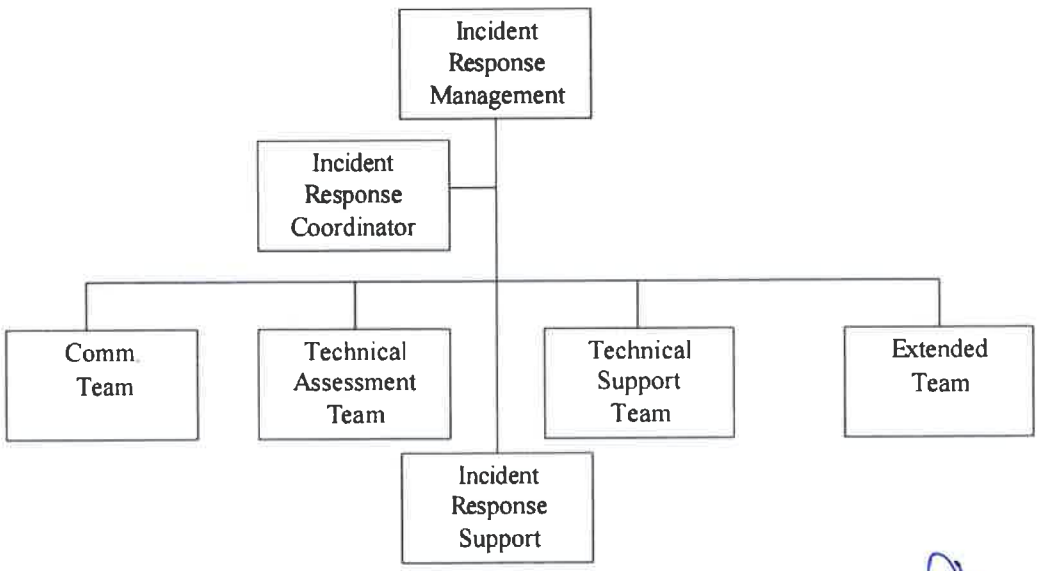
Once a restore has been performed, it is also important to verify that the restore operation was successful and that the system is back to its normal condition.

4.6 Follow-up

Some incidents require considerable time and effort. It is little wonder, then, that once the incident appears to be terminated there is little interest in devoting any more effort to the incident. Performing follow-up activity is, however, one of the most critical activities in the response procedure. This follow-up can support any efforts to prosecute those who have broken the law. This includes changing any company policies that may need to be narrowed down or be changed altogether.

5. Organization

To adequately respond to an intrusion or incident, predetermined teams will participate depending on the incident characteristics. As the situation develops and the impact becomes more significant, the various teams will be called to contribute. Figure 1 depicts the Incident Response organization.



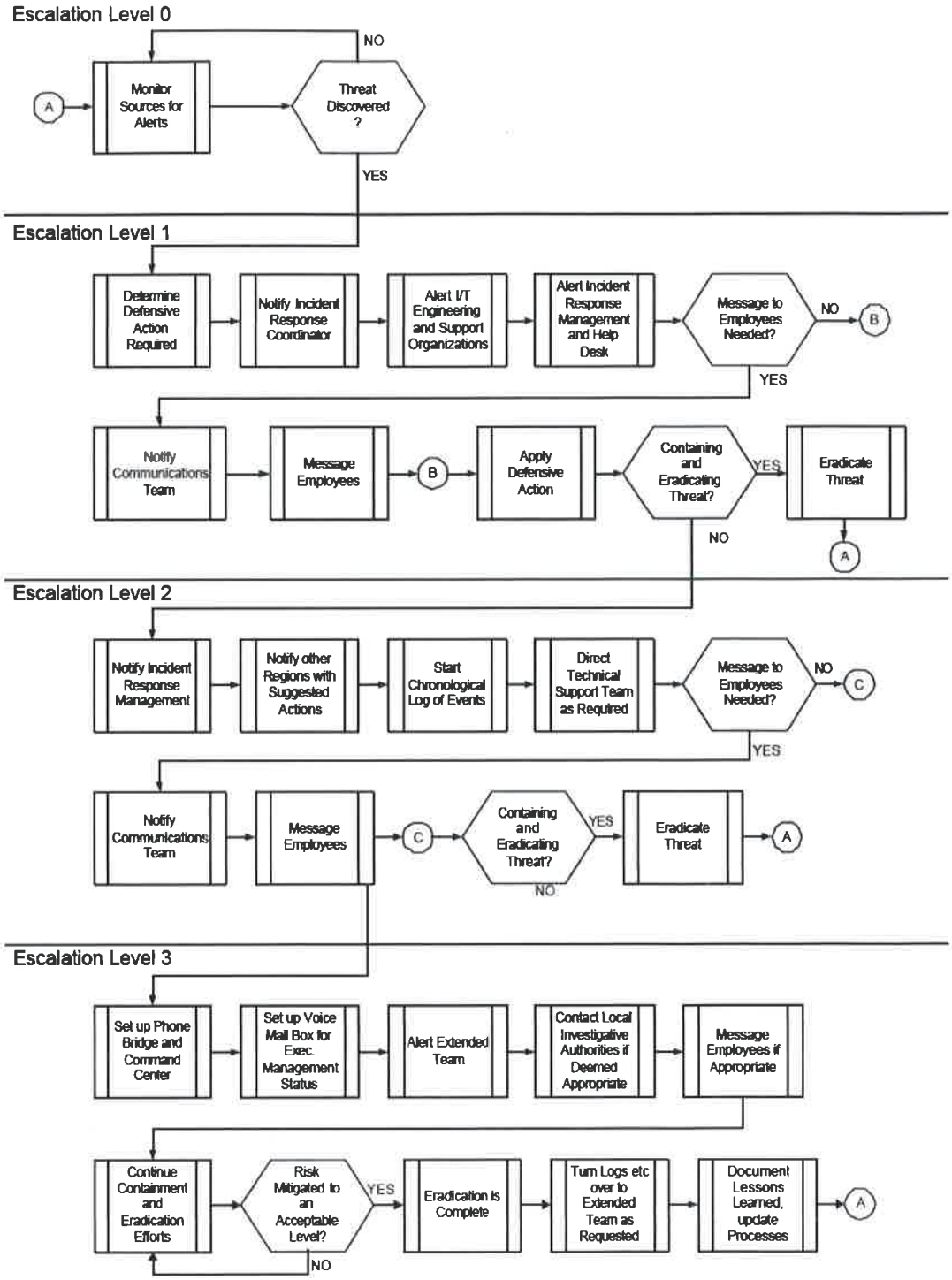
6. Escalation Levels

Whenever the impact of the incident increases (severity level increases) the escalation process will be invoked to involve all appropriate resources. Incidents should be handled at the lowest escalation level that is capable of responding to the incident with as few resources as possible in order to reduce the total impact, and to keep tight control. Following table defines the escalation levels with the associated team involvement.

Escalation Level	Affected Team(s)	Description
0	Technical Assessment Team	Normal Operations. Engineering groups monitoring for alerts from various sources
1	• Technical Assessment Team • Incident Response Coordinator • Communication Team	A threat has been discovered. Determine defensive action to take. Message employees of required actions if necessary.
2	• Incident Response Management • Incident Response Coordinator • Technical Assessment Team • Technical Support Team • Communications Team	A threat has manifested itself. Determine course of action for containment and eradication. Message employees of required actions if necessary.
3	• Incident Response Management • Incident Response Coordinator • Extended Team • Technical Assessment Team • Technical Support Team • Communications Team • Incident Response Support Team	Threat is wide spread or impact is significant. Determine course of action for containment and eradication. Message employees. Prepare to take legal action for financial restitution etc.

7. The Incident Response Process

The Incident Response Process is an escalation process where as the impact of the incident becomes more significant or wide spread, the escalation level increases bringing more resources to bear on the problem. At each escalation level, team members who will be needed at the next higher level of escalation are alerted to the incident so that they will be ready to respond if and when they are needed.


Escalation Level 0
A
Monitor Sources for Alerts
Threat Discovered ?
NO
YES
Escalation Level 1
Determine Defensive Action Required
Notify Incident Response Coordinator
Alert I/T Engineering and Support Organizations
Alert Incident Response Management and Help Desk
Message to Employees Needed?
NO
B
YES
Notify Communications Team
Message Employees
B
Apply Defensive Action
Containing and Eradicating Threat?
YES
Eradicate Threat
A
NO
Escalation Level 2
Notify Incident Response Management
Notify other Regions with Suggested Actions
Start Chronological Log of Events
Direct Technical Support Team as Required
Message to Employees Needed?
NO
C
YES
Notify Communications Team
Message Employees
C
Containing and Eradicating Threat?
YES
Eradicate Threat
A
NO
Escalation Level 3
Set up Phone Bridge and Command Center
Set up Voice Mail Box for Exec. Management Status
Alert Extended Team
Contact Local Investigative Authorities if Deemed Appropriate
Message Employees if Appropriate
Continue Containment and Eradication Efforts
Risk Mitigated to an Acceptable Level?
YES
NO
Eradication is Complete
Turn Logs etc over to Extended Team as Requested
Document Lessons Learned, update Processes
A

8. Responsibilities

A person(s) must be formally assigned the responsibility to create and distribute security incident response and escalation procedures to the necessary personnel.

Area Responsible :
Manager :
Information Security Team :

> **CAUTION**: No staff member, except the designated Information Security personal has authority to discuss any security incident with any person(s) outside of PVR Ltd.

9. Incident Response Plan Coverage

The incident response plan must include at a minimum the following

- Roles, responsibilities, and communication strategies in the event of a compromise.
- Coverage and responses for all critical system components.
- Notification, at a minimum, of credit card associations and acquirers.
- Strategy for business continuity post compromise reference or inclusion of incident response procedures from card associations.
- Analysis of legal requirements for reporting compromises.
- Data Backup and Recovery of Critical systems

10. Incident Response Escalation Mechanism

The incident response plan must define an incident escalation process. It should pre-define the personnel responsible for immediate incident response and the persons to whom the incident should be escalated in case of incident remaining unresolved.

11. Testing of Incident Response Plan

The incident response plan must be tested at least once annually. All testing results must be documented and the incident response plan must be changed depending on the testing results.

12. Incident Response Support

There should be designated security personnel who should be available 24/7 to respond to unauthorized activity, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.

Area Responsible :
Manager :
Information Security Team :

13. Training

The staff providing incident response must be appropriately trained to respond to security breaches. Training requirements must be accessed on the basis of incident response plan testing and performance of incident response personnel.

14. Alerts

An alerting mechanism must be in place to notify the incident response personnel. The alerts to be sent to incident response personnel must include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.

Typical symptoms of computer security incidents include any or all of the following:

- A system alarm or similar indication from an intrusion detection tool
- Suspicious entries in system or network accounting
- Accounting discrepancies
- Repeated unsuccessful logon attempts
- Unexplained, new user accounts
- Unexplained new files or unfamiliar file names
- Unexplained modifications to file lengths and/or dates, especially in system executable files
- Unexplained attempts to write to system files or changes in system files
- Unexplained modification or deletion of data
- Denial/disruption of service or inability of one or more users to login to an account
- System crashes
- Poor system performance
- Operation of a program or sniffer device to capture network traffic
- Remote requests for information about systems or users (e.g., social engineering)
- Unusual time of usage (many computer security incidents occur during non-working hours)
- An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user
- Unusual usage patterns (e.g., programs are being compiled in the account of a user who does not know how to program, an escalation in disk usage by a single account)

15. Incident Response Plan Updating

There must exist a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. Annual Security Incident Response Test Procedure can be used for this purpose. Any lesson-learned during the test phase must be incorporated into the Production Procedure.