Marquistech – Security Incident Response Procedure

Owner	:	Information Security Officer
Reviewer	:	Sudarshan Kadam
Approver	:	Deven Potdar
Version & Status	:	1.4, Approved

1 Purpose

The Security Incident Response Procedure is intended to communicate what is expected of personnel when confronted with an incident pertaining to resource confidentiality, integrity, and/or availability. The policy is also pertains to triggering an security incident in case of loss or misuse of organizational properties. The policy provides the vital framework necessary to develop detailed incident response procedures. This document discusses the procedures followed during an incident response.

2 Scope

This policy applicable to all employees, contractors, and consultants who handle Marquis Technologies assets including those who have access to sensitive information or sensitive information entrusted to Marquis Technologies.

3 Policy Statement

1) The person who discovers the incident will call one of below. List possible sources of those who may discover the incident. The known sources should be provided with a contact procedure and contact list. Sources requiring contact information and to be contacted are:
    a) Reception
    b) Team Lead
    c) IT Department
    d) A manager
    e) Corporate Security
2) If the person discovering the incident is a member of the IT department or affected department, they will proceed to step 5.
3) If the person discovering the incident is not a member of the IT department or affected department, they will call the 24/7 reachable Corporate Security No. +91-9664176756 or IT Department No. +91-9167799360
4) The Corporate security or the IT Department will log:
    a) The name of the caller.
    b) Time of the call.
    c) Contact information about the caller.
    d) The nature of the incident.

e) What equipment or persons were involved?

f) Location of equipment or persons involved.

g) How the incident was detected.

h) When the event was first noticed that supported the idea that the incident occurred.

5) The Corporate security or the IT Department who receives the call (or discovered the incident) will form the Incident Response Team (IRT) with HR and Project Managers. The IRT will log the information received in the same format as the grounds security office in the previous step. The IRT could possibly add the following:

   a) Is the equipment affected business critical?

   b) What is the severity of the potential impact?

   c) Name of system being targeted, along with operating system, IP address, and location.

   d) IP address and any information about the origin of the attack.

6) The IRT will meet or discuss the situation over the telephone and determine a response strategy.

   a) Is the incident real or perceived?

   b) Is the incident still in progress?

   c) What data or property is threatened and how critical is it?

   d) What is the impact on the business should the attack succeed? Minimal, serious, or critical?

   e) What system or systems are targeted, where are they located physically and on the network?

   f) Is the incident inside the trusted network?

   g) Is the response urgent?

   h) Can the incident be quickly contained?

   i) Will the response alert the attacker and do we care?

   j) What type of incident is this? Example: virus, worm, intrusion, abuse, damage.

7) An incident ticket will be created. The incident will be categorized into the highest applicable level of one of the following categories:

   a) Category one - A threat to public safety or life.

   b) Category two - A threat to sensitive data

   c) Category three - A threat to computer systems

   d) Category four - A disruption of services

8) IRT members will establish and follow one of the following procedures basing their response on the incident assessment:

a) Cyber Threat response procedure
b) System failure procedure
c) Property theft response procedure
d) Prototype Theft or Loss response procedure.

The team may create additional procedures which are not foreseen in this document. If there is no applicable procedure in place, the team must document what was done and later establish a procedure for the incident.

9) IRT members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization.
10) IRT members will recommend changes to prevent the occurrence from happening again or infecting other systems.
11) Upon management approval, the changes will be implemented.
12) IRT members will restore the affected system(s) to the uninfected state. They may do any or more of the following:
    a) Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
    b) Make users change passwords if passwords may have been sniffed.
    c) Be sure the system has been hardened by turning off or uninstalling unused services.
    d) Be sure the system is fully patched.
    e) Be sure real time virus protection and intrusion detection is running.
    f) Be sure the system is logging the correct events and to the proper level.
13) Documentation—the following shall be documented:
    a) How the incident was discovered.
    b) The category of the incident.
    c) How the incident occurred, whether through email, firewall, etc.
    d) Where the attack came from, such as IP addresses and other related information about the attacker.
    e) What the response plan was.
    f) What was done in response?
    g) Whether the response was effective.

14) Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.
15) Notify proper external agencies—notify the police and other appropriate agencies if prosecution of the intruder is possible. List the agencies and contact numbers here.
16) Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.
17) Review response and update policies—plan and take preventative steps so the intrusion can't happen again.
    a) Consider whether an additional policy could have prevented the intrusion.
    b) Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.
    c) Was the incident response appropriate? How could it be improved?
    d) Was every appropriate party informed in a timely manner?
    e) Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?
    f) Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
    g) Have changes been made to prevent a new and similar infection?
    h) Should any security policies be updated?
    i) What lessons have been learned from this experience?

4 Contact

The Primary Contacts for any Security Incidents are:

Deven Potdar – IT Manager

Email - dpotdar@marquistech.com

Mobile - +91 9167799360

Abel Subhash – Corporate Security

Email - asubhash@marquistech.com

Mobile - +91 9664176756

5 Policy Review and Revision History

Version	Reviewer	Date
1.0	Deven Potdar	10-06-2019
1.1	Deven Potdar	12-12-2020
1.2	Sudarshan Kadam	09-10-2021
1.3	Deven Potdar	14-11-2023
1.4	Deven Potdar	19-11-2024