May's Marvellous Mice Again

Incident Management

December 15, 2021

Table of Contents

Incident Management

It is critical to the organization that security incidents that threaten the security or confidentiality of information assets are properly identified, contained, investigated, and remediated.

May's Marvellous Mice Again Incident Management Policy

1.0 Purpose

The purpose of this policy is to provide guidelines to manage security incidents that threaten the confidentiality, integrity or availability of information assets.

2.0 Scope

The policy applies to all employees, consultants and contractors of May's Marvellous Mice Again. This policy is also applicable to all types of incidents (including but not limited to ones defined in this policy) related to information assets such as IT systems/services and related support systems of May's Marvellous Mice Again.

3.0 Definitions

Information security event: Any occurrence related to information assets or the environment indicating a possible compromise of policies or failure of controls or an unmapped situation that can impact security.

Information security incident: Any event that threatens the confidentiality, integrity, or availability of organization systems, applications, data, or networks. Examples of organization systems include, but are not limited to:

- Servers
- Desktop computers
- Laptop computers
- Workstations
- Mobile devices
- Network equipment

Examples of security incidents include, but are not limited to:

- Unauthorized access
- Potential violation of May's Marvellous Mice Again approved policies
- Potential data and privacy breach
- Intentionally targeted but unsuccessful unauthorized access
- Accidental disclosure of confidential data
- Infection by malware
- Denial-of-Service (DoS) attack
- Theft or loss of an organization system or asset
- The theft or physical loss of computer equipment
- Loss or theft of tablets, smartphones or other mobile devices
- A server known to have sensitive data is accessed or otherwise compromised by an unauthorized party
- A firewall accessed by an unauthorized entity
- A DDoS (Distributed Denial of Service) attack
- The act of violating an explicit or implied security policy
- A virus or worm uses open file shares to infect from one to hundreds of desktop computers
- An attacker runs an exploit tool to gain access to a server's password file
- Any event that affects the availability of our product or service
- Any event that compromises the contractual commitments to our clients

- Failure of information security controls with a likelihood of disrupting business operations

4.0 Policy

There shall be a designated individual responsible for establishing information security incident management within the organization, i.e., overseeing incident management activities, including documentation, response, escalation, resolution and analysis of incidents.

May's Marvellous Mice Again should communicate where applicable with its employees, customers and other stakeholders when an incident that impacts them occurs, provide updates during the incident and after the resolution.

As needed, the security incidents would be reported outside of May's Marvellous Mice Again by a designated person nominated by senior management. Users shall not report to or discuss incidents with other users or external persons as this may affect the May's Marvellous Mice Again ’s reputation or hinder the investigation.

Intrusion attempts, security breaches, theft or loss of hardware, suspicion of an incident or other security-related incidents perpetrated against the organization must be reported to the incident management team (See Appendix A for details). All known vulnerabilities, in addition to all suspected or known violations, must be communicated in a timely manner.

The team responding to the incident shall keep notes and use the appropriate chain of custody procedures to ensure that the evidence gathered, both digital and physical, during the security or privacy incident can be used successfully during prosecution, if appropriate. The chain of custody process should answer the following questions:

- **What is the evidence?**: For example- digital information includes the filename, md5 hash, and Hardware information includes serial number, asset ID, hostname, photos, description.
- **How did you get it?**: For example - Bagged, tagged or pulled from the desktop.
- **When it was collected?**: Date, Time
- **Who has handled it?:** Name of person
- **Why did that person handle it?**: Justification on the appropriateness of the individual handled it.
- **How it was stored?**: For example- in a secure storage container.
- **Where was it stored?**: This includes the information about the physical location in which proof is stored or information of the storage used to store the forensic image.
- **How you transported it?**: For example- in a sealed static-free bag or a secure storage container.
- **Who has access to the evidence?**: This involves developing a check-in/ check-out process.

The post-incident analysis must take place, as necessary, to identify the root cause of the incident.

All critical servers should be monitored to ensure that users only perform authorized actions and processes. Aspects to be monitored are audit trails, which record exceptions and other relevant events. Audit trails shall be kept for a defined period to assist in investigations and ongoing access-control monitoring. Access to these audit logs shall be restricted to authorized individuals only.

Accurate computer system clocks are essential to ensure the accuracy of audit logs, which may be needed for investigations or as evidence in legal or disciplinary cases.

Lessons learned from incidents shall be incorporated into May's Marvellous Mice Again’s risk assessment process for the purpose of continual improvements.

4.1 Reporting an Incident

Any breach of information security policies must be reported as soon as possible.

Users should immediately report all incidents pertaining to information security with the below information at a minimum:

- Incident Date/Time
- Type of Incident
- Description/Incident details
- Incident Location
- Contact Details

4.2 Handling an Incident

The designated personnel handling security incidents, whether an incident needs to be handed over and dealt with by departmental representatives or the incident needs to be escalated to senior management.

Upon receiving notification, the information security team will assess the severity of the incident according to the threshold in the table below:

Severity of Incident	**Criteria**	
	Users Affected	**Violation of Legal/Contractual Obligations**
Low	1 to 10	No
Medium	11 to 50	No
High	More than 50	Yes

The User affected number varies with organizations and is subject to change

Based on the severity of the incident, the designated individual will decide whether an incident needs to be “handed” over and dealt with by departmental representatives, where appropriate, or whether the incident needs to be escalated to senior management.

Representatives looking into security breaches will be responsible for updating, amending and modifying the status of incidents. The root cause of the incident must be analyzed to ensure necessary steps are taken to prevent a recurrence.

4.3 Post Mortems

The authorized personnel handling security incidents must schedule and host a post mortem using May's Marvellous Mice Again Post mortem form to ensure an appropriate post mortem is held no later than 72 hours after the incident has been completed. This post mortem must include a cross-functional team with participation from the customer success organization. The goals of the post mortem at a high level are:

- To find a Root Cause
- To prevent recurrence
- To understand the level of impact and missed Service-level agreements (SLA)
- To provide the Customer Success team all the information and collateral to communicate with customers, as required

Appendix 1

Contact details for incident reporting

Incident Category	**Contact Person**	**Email Address**	**Phone Number**
Physical and Environmental			
IT and Security			
Data Breach and Privacy			

General Emergency	**Call 911**