DoControl.

One SaaS to secure all other SaaS

Information Security Management System
Edition 1.1 | Sept 13, 2020

Security Incident Handling

1. Objective

This procedure outlines the controls, processes and guidelines that apply upon the suspected deviations from the normal state of information security, its policy or otherwise the company development and rendering services to customers.

2. Definitions

The following events at minimum are considered Security Incidents:

a. Suspected malware impact on servers / workstation
b. Any sort of unauthorized access to systems or data
c. Multiple failed login attempts or actual account lockouts
d. Significant latency in the network or service delivery
e. Identification of unknown/unexplained files, traces, error messages
f. Physical break-in to facilities with or without theft of assets
g. Impersonation, phishing or fraud attempts
h. Any other suspicious or abnormal behavior

3. Ownership & Responsibility

1. The CTO is responsible for the overall confidentiality, integrity and availability of the company's computing and networking assets.
2. The Information Security Manager is responsible to aid the CTO in responding to all security incidents in order to reduce potential damage.
3. The Information Security Manager is also responsible for this procedure.

4. Method

1. Employees are expected to report on any suspected security incident or behavior.
2. Security is responsible for performing initial assessment of each reported incident to determine its risk and impact.
3. Security incidents will be clearly documented and include all required information for providing visibility to management as well as to efficiently handle and contain the issue.
4. As part of the incident handling, all applicable pieces of evidence will be gathered and securely handled.

5. A process of drawing conclusions will be executed, while defining activities for prevention of events of this kind in the future.

6. Malware, phishing and unauthorized access attempts require immediate response, escalation and reporting.

7. Users with malware infection are expected to disconnect from any network and contact Security as soon as possible, to check if this is an isolated issue or has an impact on other assets.

8. In case the company cannot handle the incident on its own resources, it will engage an incident response and forensics firm to aid in the process.

9. In cases where it is discovered that the incident was caused in consequence of negligent work of employees of the Company, disciplinary actions against the employee ought to be contemplated.

10. System owners are responsible to escalate to Security and initiate an Incident Response procedure anytime they suspect there’s an issue with systems or services under their ownership.

11. Incidents requiring coordination with several owners or teams will be managed in a war-room mode (virtual or physical), with periodical updates and status meetings until resolution.

12. Communication aspects are to be discussed and determined following an update with the company leadership including Legal and senior management.

13. Communicating incidents to the public is subject to law and regulations requirements. Any such communication is subject to that CEO and Board of Directors approval and so does the decision on who is authorized to be interviewed by the media or reporters.

5. Document Revision History:

AUTHOR	Edition	COMMENTS	DATE
Ron Peled, Security Consultant	1.0	First draft	
Ron Peled, Security Consultant	1.1	Adjustments to DoControl	

6. Approvals

NAME	TITLE	E-SIGNATURE	DATE
Liel Ran	CTO		Sep 15, 2020