Incident Management Policy

1. Introduction

Avoidance of potential computer security incidents require the implementation of solid security policies. Measures include blocking unnecessary access to networks and computers, improving user security awareness and early detection & mitigation of security incidents to significantly reduce the risk of security incidents and allow.

This document describes the requirements for dealing with computer security incidents. Security incidents include, but are not limited to: virus, worm, and Trojan horse detection; unauthorized use of computer accounts and computer systems; as well as complaints of improper use of Information Resources.

NetFM's Incident Management Policy applies equally to all and any individuals that use or have access to any NetFM Information Resources (IR).

2. Definitions

Information Resources (IR): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, removable media (e.g. USB devices), personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources Manager (IRM) (The Technical Director)**:** Responsible for management of the company's information resources. The designation of an company Information Resources Manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the company's information activities, and ensure greater visibility of such activities within and between the company and clients. The IRM has been given the authority and the accountability by the Company to implement Security Policies, Procedures, Practice Standards and Guidelines to protect the Information Resources of the Company and its clients. If the Company does not designate an IRM, the title defaults to the Company's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

Security Incident: In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent**.**

3. Incident Management Standard Practice

- Any member of NetFM discovering an incident has defined duties to fulfil and responsibilities which can take priority over normal duties.
- Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate Incident Management procedures must be followed.
- The member of NetFM discovering the incident is responsible for notifying the Technical Director and initiating the appropriate incident management action as defined in the Incident Management Procedures.
- The Technical Director (in their role as the IRM / ISO) is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
- The appropriate technical resources required will be provided by the company ensure that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized wherever possible.
- The Technical Director will determine whether communication to all members of the company is required, the content of the communication, and how best to distribute the communication.
- The Technical Director will ensure that the appropriate technical resources are available to all employees to communicate new issues or vulnerabilities to the Technical Director to liaise with relevant personnel to eliminate or mitigate the vulnerability.
- The Technical Director is responsible for initiating, completing, and documenting the incident investigation with assistance from the NetFM employee discovering the incident.
- The Technical Director is responsible for coordinating communications with external organisations and law enforcement.
- In the case where law enforcement is not involved, the Technical Director will recommend disciplinary actions, if appropriate.
- In the case where law enforcement is involved, the Technical Director will act as the liaison between law enforcement and NetFM Ltd.

4. Disciplinary Actions

Violation of this policy may result in disciplinary action, which may include termination for employees and temporaries or a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of NetFM Information Resources access privileges, civil, and criminal prosecution as appropriate.