Incident Management Policy & Procedure

1 Overview

This policy establishes governance over Information security incident management, and includes monitoring, reporting and responding to security incidents. All system users are responsible to PRESERVE the security of their work environment by reporting suspected IT security breaches or incidents as described in this policy.

2 Purpose

This policy seeks to:

2.1 provide governance over the management of Information security incidents including monitoring, reporting and response processes and procedures;

2.2 limit the potential for Information security incidents to adversely impact business continuity through loss, damage, disruption or unauthorized access to information and IT services;

2.3 increase WELDO user awareness in relation to security incidents; as well as provide information on user responsibilities for reporting IT security incidents.

3 Scope

This policy applies to all users of the WELDO's facilities and equipment including staff and any third party suppliers and contractors.

4 Policy

WELDO will manage security incidents, including virus outbreaks, unauthorized access and system compromises; denial of service or other incidents through the procedure mentioned in this document.

Refer to: *Security Incident Management Procedure – Annex A*

WELDO reserves the right to monitor access and investigate account, computer systems and network usage for the purposes of managing incidents and determining (where it has reasonable cause to suspect), non-compliance with security policy. WELDO also reserves the right to isolate areas of the network, disconnect any computer, voice, video or network equipment and block file types in order to contain security incidents.

4.1 Definition of IT Security Breach or Incident

A security breach or incident includes the following:

4.1.1 Unmanaged viruses, worms or malicious code.

4.1.2 Unauthorized access attempts (hacking);

4.1.3 Unauthorized network and port scanning;

4.1.4 Unauthorized connection of computer, video, voice or other network equipment

4.1.5 Material that infringes copyright;

4.1.6 Denial of Service (DOS) attacks;

4.1.7 Web site defacement;

4.1.8 Theft, misuse or critical loss of IT resources including equipment, system information or login identities/passwords;

4.1.9 Unauthorized work practices that are directly non-compliant with information security related policy or accepted codes of practice;

4.1.10 Spam email containing unmanaged malicious content or attachments;

4.1.11 Electronic threatening, harassing, obscene or offensive messages;

4.1.12 Any other suspicious activity, event or situation related to security of information or information systems.

4.2 Incident Reporting

All IT security incidents and breaches (as per the definition above) must be reported to the WELDO Data Protection Officer.

All suspected incidents must be reported to the following:

1. Send email to dpo@weldo.org

Warning: If reporting a suspected security weakness or system vulnerability, do not attempt to confirm it by testing the weakness since that could be interpreted as a potential misuse of the system or cause damage to it.

Ms. Sijal Aziz

Data Protection Officer

E-mail: dpo@weldo.org

The following information (where known) must be reported: (as per Incident Reporting

Form, attached as annexure)

- General nature of the security incident;
- Systems involved in the incident;
- Impact or potential/impact of the incident;
- When the security incident occurred;
- Details of any person/s directly involved in the incident;
- How the security incident occurred;
- Possible preventative measures for control.

IT security incidents and breaches must not be broadcasted or publicized outside of the organization as this may increase associated risk. Broadcast or widespread publicity will result in increased risk to the integrity of IT services and systems and constitutes a breach of policy.

4.3 Incident Response

The WELDO DPO, when alerted to a security incident or breach, will activate the Security Incident Management procedure *(Refer to Security Incident Management Procedure – Annex A)* and undertake the following lifecycle process:

- Analysis
- Containment
- Eradication and Recovery
- Follow-up

Incidents and breaches may be dealt with through internal or external processes or a combination of both. Internal processes may include relevant partner policies, statutes, rules, orders and disciplinary processes.

Where incidents result in a reasonable case established in relation to non-compliance to policy, the organization may undertake the following:

- WELDO may monitor any account, computer or IT system without notice;
- WELDO may inspect without notice any data on any partner computer, system or network including electronic mail and other forms of communication regardless of data ownership;
- WELDO may temporarily suspend or permanently cancel IT system accounts;
- WELDO may disconnect any or all unauthorized computer, video, voice or other network based equipment;
- WELDO and / or HR Department may apply appropriate sanctions against offenders;
- WELDO may issue a 'Take Down' notice for infringing material, which may further result in disciplinary action.

4.4 Enforcement

WELDO may immediately disconnect any unauthorized equipment, suspend accounts, access and any person from using IT facilities and services (and may recommend further penalties to the HR Department, up to and including employment sanctions and legal action) if after appropriate investigation a person is found to:

- Be responsible for theft of IT equipment or willful damage to any IT equipment, facilities, systems or information;
- Be in unauthorized possession of confidential information obtained improperly;
- Be responsible for deliberate or careless interruption of IT services;
- Have gained unauthorized access to accounts, passwords, systems or information or IT processing facilities;
- Have shared accounts or passwords without authorization;
- Be responsible for connection of unauthorized computer, video, voice or other network equipment
- Have possession of or be responsible for acts of infringing material (including copyright or offensive material);
- Be knowingly aware of and/or have observed inappropriate behavior and have failed to report this;
- Be responsible for any security incident as per the definition of this policy;
- Have been non-compliant to any part of this or any other IT related policy.

4.5 Privacy

Users have a legitimate right and expectation to privacy, however in the event where there is a reasonable case established in relation to non-compliance of policy, WELDO is not required to but reserves the right to, within allowable legal parameters, monitor information systems, record monitored events and respond to and provide evidence in the case of unauthorized activities or other security incidents that contravene acceptable use as defined through Information Technology security policies, practices and procedures. The effect of this be immediately brought in the notice of DPO.

Annexure Security Incident Management Procedure

1 Incident Handling and Response

Security incident response will be typically handled through several stages: analysis, containment, eradication and recovery, and follow-up.

1.1 Analysis

Once a potential security incident is reported or anomalous activity detected, analysis must be performed to determine if it is indeed symptomatic of a security incident and to understand the nature of the incident for proper remediation.

1.1.1 Goals

a) Understand the nature and scope of the incident

b) Collect enough information about the incident so the response team can prioritize the next steps in handling the incident, which is normally containment

c) Determine if confidential data is involved in the incident

1.1.2 Components of security incident analysis

a) Collaboration with other professionals as needed (for example, a security analyst, network analyst, system administrator, and application manager working as a team to analyze the system exhibiting the anomalous behavior; relevant WELDO representative; consulting external sources like REN-ISAC, US-CERT, SANS, etc.)

b) Understanding normal system and network behavior so anomalous activity can be identified

c) Analysis and correlation of as many indicators as possible, such as monitoring network traffic to/from the host suspected of being compromised, network packet captures for more in-depth analysis, IPS / Firewall / Server log file analysis, interviews with users and/or system administrators, etc.

d) Initial determination of the incident's scope (How many systems affected? Is it actively propagating? If so, how?)

e) Research of the specific malware or type of attack

f) Collection of additional data which may require permission from the DPO

1.1.3 Procedures for Analysis

a) Detect security event

b) Analyze event data to determine if it is indicative of a security incident and get an initial impression of the nature and scope of the incident

c) Notify the DPO who may assist with the initial analysis of the event data. Other appropriate personnel may be notified at this point as well, like relevant IT support staff, the WELDO IT Manager, or a supervisor or department head.

d) The DPO will record it in the Incident Tracking System (see section 3.1 below)

e) If there's a need to access personal data, like an individual's e-mail or files, in order to gather more information about the incident, first get approval from the DPO.

f) Determine if any confidential data was or might have been affected.

g) If the incident is of high or medium severity:

i. Image the hard drive, memory, and any other relevant media before performing analysis that might alter evidence. For hard drives, bit-by-bit copies are required in case deleted files need to be recovered. This is especially important for cases that involve confidential data, possible criminal investigation, or sensitive personnel actions.

ii. Preserve the original media in a secure location and perform analysis on a copy of the data.

iii. Take notes on all actions taken.

h) Perform additional forensics sufficient to characterize the incident (for example, analyze netflow data).

1.2 Containment

Once a security incident in confirmed, the next step is typically containment.

1.2.1 Goals

a) Stop potential loss of confidential data
b) Protect other computers and information on the network and Internet (for example, keep the malware from spreading to other computers on or off site)
c) Prevent further damage to the compromised system and/or information
d) Identify the location and owner of the computer(s) so they can be engaged in containment, eradication, and recovery

1.2.2 Delaying containment

In some cases, containment may need to be delayed in order to monitor the attacker's activity, usually to collect more evidence. However, the risk of the compromised system being used to attack other systems or breach confidential data could lead to legal liabilities. Consult with the Head of InfoSec before deciding to delay containment.

1.2.3 Procedures for Containment

a) Identify the location and/or owner of the system(s) involved in the incident by checking any of the following:
    a) Network ARP tables to map the IP address to a MAC address
    b) DHCP logs for MAC address and hostname
    c) "nbtscan" command to query host NetBIOS information
    d) Active Directory for registered user computers
    e) "CSMARS" network device management software
    f) Kaspersky Antivirus Management Console
b) Determine if the computer needs to have its network access blocked. If so, this can be accomplished in several ways by the WELDO network team:

    i. At the switch port, router interface, network border ii. Block the MAC address on all campus wireless networks (be sure to block it on all wireless networks. Also block the wired network interface for the same computer if known. Iii. Disable VPN access

c) An alternative to blocking all network access, if available, is to put the computer in a network quarantine by using Kaspersky Antivirus Management Console.

d) There may be cases when a specific protocol or UDP/TCP port needs to be blocked at the network border or some other network interface in order to prevent propagation of the malware or to protect the network

from further attacks. This can be achieved at the firewalls or router Access Control Lists.

e) Notify the IT Manager and/or user responsible for the system.

f) Isolate the affected computer(s) either by unplugging the network cable (preferred) or shutting down the computer. Unplugging the network cable and leaving it running is best since shutdown can alter or destroy evidence, like with memoryresident malware. For wireless computers, the wireless interface can be disabled while leaving the computer running.

g) Perform containment on the affected system(s) to keep it(them) from doing further damage to the computer or the data on it. This step depends on the nature of the compromise/malware, the need for preserving evidence (i.e., if you have to preserve evidence, don't do anything to the computer until images of RAM and the hard drive are captured), the urgency of restoring the service hosted on the affected systems, and the time and resources available.

1.3 Eradication and Recovery

1.3.1 Goals

a) Preserve evidence if it has not already done
b) Perform additional analysis as needed to complete the investigation
c) Remove the components of the incident impacting the affected systems, such as deleting the malicious code or disabling a compromised user account.
d) Mitigate the attack vector so a similar incident does not occur (for example, patch the vulnerability used to compromise the system, apply standard system hardening procedures, adjust firewall rulesets, etc.)
e) Restore systems to normal operation

1.3.2 Procedures for Eradication and Recovery

a) Determine the full scope of the incident – how many systems did it affect and therefore need to be repaired?
b) Determine if any additional analysis is needed:

i. Determine if any of the affected systems still need to have memory, hard drive(s), or other media imaged to preserve evidence; make an image copy of the media, preserve the original and perform analysis on the copy. ii. Perform additional analysis, which may include:

- Searching for malware by running an anti-virus scan and/or rootkit detection software, or looking for specific files known to be associated with current threats
- Recover deleted files and file fragments
- Perform a vulnerability scan
- Check for unusual running processes and suspicious registry entries, especially ones that run on start-up
- Determine open network ports and processes listening to those ports
- Take a network packet capture and analyze the network traffic
- Analyze network flow data

- Analyze log files for unusual activity
- Search for confidential data that may have been missed in the initial analysis

c) Determine if a reformat/reinstall is required. Compromises that allow remote control of the system, gain root/Administrator privileges, and/or install a backdoor require a complete, clean re-install of the system for eradication.

i. The DPO in conjunction with IT Manager will determine when a specific type of compromise requires reformat/reinstall

ii. Reformatting the hard drive and re-installing from a backup tape prior to the compromise is acceptable, as is restoring from a clean image for those systems that use disk imaging technology like Symantec Ghost.

iii. Note that reinstalling must occur without exposing the vulnerable system to the network and the Internet

d) If infected with malware and a reformat/reinstall is not required, remove the malware from the system. Running an anti-virus scan after updating virus definition/pattern file may suffice. Specific instructions for removing certain types of malware may also be found by searching the Internet.

e) Mitigate the attack vector to prevent further instances. This may include:

i. Patching vulnerabilities in the operating system and all applications software

ii. Changing passwords

iii. Adjusting firewall rules iv. Updating or installing new security software (for example, anti-virus software or a host-based personal firewall)

iv. Applying standard system security hardening techniques

v. Passing a security assessment

vi. User training

f) Restore network access if the system was blocked during the containment phase. The request to remove the network block must come from the appropriate WELDO representative in as described here.

g) Return the system to normal operations

1.4 Follow-up

1.4.1 Goals

a) Determine lessons learned and make recommendations to prevent subsequent similar incidents

b) Issue final reports

c) Archive evidence and documentation

d) Close out the incident

1.4.2 Procedures

a) The DPO should confirm that all action items, investigations, analyses, and communications are completed

b) Hold a Post-Incident Review session, if required, to determine ways to improve WELDO's management of security incidents and help prevent future incidents, not to assign blame.

i. It should be scheduled to occur within 2-3 weeks of the incident's remediation

ii. Include the incident response team and relevant stakeholders

iii. Appoint one person to record notes – successes, failures, recommendations, and action items

iv. Cover the following areas in the review session:

- Are there any open issues? In other words, is remediation of the incident complete?
- What could have prevented the incident?
- How effectively was the incident handled (response time, communication, following procedures, containing spread/damage, etc.)?
- Recommend changes to policy, procedure, and security controls to prevent and more effectively handle future incidents.
- Identify any needed follow-up tasks and assign those tasks to individuals

c) Evidence management – does any evidence need to be preserved longer? If so, for how long and by whom? Release or properly destroy any evidence that is no longer needed.

d) Complete a Post-Incident Report if required (see "Post-Incident Report" in section 3.3 below) and submit it to the DPO. Security incidents with a severity category of "high" must complete a post-incident report. The DPO may request a post-incident report for any security incident.

e) The DPO will review any recommendations and consider assigning resources to implement them.

f) Archive reports and other relevant documents and communications ("work product"). This includes log files, timelines, recovered files, notes, network flow data, e-mails, etc.

g) Close out incident tickets in the incident tracking system

2 Collection and Preservation of Evidence

When a security incident involves legal action against a person or organization, or a personnel action against an WELDO employee, evidence must be collected, preserved, and presented to conform to the rules for evidence specified in the relevant jurisdiction(s). The following procedures help ensure the strong evidence trail needed for admissibility (making sure it can be used in court) and weight of evidence (high quality and completeness).

2.1.1 When collecting evidence, follow all appropriate WELDO policies and procedures, such as getting permission from the DPO to access data.

2.1.2 Document all actions taken in the collection and preservation of the evidence.

2.1.3 For data stored on electronic media, such as a hard disk drive, USB flash drive, CD, DVD, or RAM, make a mirror image or copy (depending on applicable requirements) of the media. For example, if forensics will require recovering deleted files or file fragments from a hard drive, a bit-by-bit mirror image of the drive is required since a file-by-file copy will not capture that data.

a) Have another person witness the imaging/copying process. If the incident involves a high profile or sensitive criminal case, have a law

enforcement officer assist with the collection of the evidence, witness the imaging/copying process, and store the originals.

b) Log all actions taken during the imaging/copying process, including date, time, and location the image/copy was made, who performed the actions and who witnessed it, and the tools and programs used.

c) Label the original media and store it along with the log of the imaging/copying process in a secure location.

2.1.4 Perform all forensics work on the image or copy, not the original. Additional images or copies of the original can be made if needed (for example, if forensics analysis on the copy destroyed some evidence and you need to continue analysis on a fresh copy).

2.1.5 For paper-based documents, keep the original in a secure location and log the following:

a) who found the document
b) where it was found
c) date and time it was found
d) who witnessed the discovery

3 Incident Tracking and Reports

3.1 Incident Tracking System

3.1.1 The Head of InfoSec will maintain an incident tracking system and record the following information about all reported security incidents:

a) Incident ID number assigned by the Head of InfoSec in the form YYYY-XXX where “YYYY” is the year in which the incident occurred and “XXX” is a unique number that roughly corresponds to the sequential order of occurrence of the incident that year. For example, 2007-103 would be the 103rd incident that occurred in 2007.
b) Incident category(ies), severity, and description
c) Identity of the affected system(s) – IP address, domain name, MAC address
d) Whether the system contains confidential data
e) Location of the affected system(s) – building and department
f) Contact information – usually the departmental security contact, appropriate system administrator, or WELDO representative
g) Dates and times – first notice, when contact notified, blocking/unblocking
h) Recovery action taken

3.1.2 All IT security incidents or suspected incidents (i.e., reports of suspicious activity that upon investigation are determined not to be a security incident) will be recorded in the incident tracking system.

3.1.3 The incident tracking system should be used to identify trends or outbreaks that may require changes to security controls and/or policies to reduce the risk of future occurrences.

3.1.4 The incident tracking data is considered confidential and should therefore be encrypted when stored or transmitted and disclosed only to authorized individuals. The confidentiality of reports derived from the incident tracking data will be determined on a case-by-case basis by the Head of InfoSec and/or the CIO.

3.2 Annual Report

3.2.1 In January each year, the DPO will summarize the incidents for the previous calendar year and provide a report to the WELDO Management. The security incident data may also be used for other reports as needed. This report will be marked as confidential.

3.3 Post-Incident Report

3.3.1 Individual security incidents may require completion of a Post-Incident Report. Incidents with a severity category of “high” must submit one, and the DPO may request one for any security incident.

3.3.2 The DPO will review any recommendations in the report and determine additional follow up actions.

3.3.3 Post-incident reports must be submitted to the DPO and be marked as confidential.