INCIDENT MANAGEMENT PROCEDURE

Document Number: CF-IM-PR-01

Version Number: 1.02

Release Date: 2nd February 2021

Prepared by	Reviewed by	Approved by
Name: Kirk Bushell Designation: Technical Director	Name: Richard de Nys Designation: MD	Name: Richard de Nys Designation: MD
Date: 03-Oct-2017	Date: 05-Oct-2017	Date: 05-Oct-2017

Document Revision History

Date	Version Number	Brief Description of change	Change Request Number
03-Oct-2017	1.00	Initial Release	NA
17-Aug-2020	1.01	Company name amendment	NA
02-Feb-2021	1.02	NC Closure	NA

Table of Contents

1 Purpose

The purpose is to define the procedure for handling all incidents that have an impact on Creative Force's information assets and resources within the scope of the Creative Force's Information Security Management System.

2 Scope

This procedure is applicable to all projects and functions at Creative Force.

3 TERMS AND DEFINITIONS

3.1 Information Security Event

Identified occurrence of a system, service or network state, indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant

3.2 Information Security Incident

Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

4 Entry Criteria

- Incident reported by any of the Creative Force employees, trainees, students, Contractors or customers.

5 Inputs

- Information security policies and procedures

6 Procedure

6.1 Incident Identification

- All the incidents that could result in the actual or potential loss of information, breaches of confidentiality, unauthorized access or changes to systems shall be reported immediately who notices it before taking any actions. (Refer Appendix- A for type of incidents)
- The incident shall be reported to CISO through any of the mode like email, phone, SMS etc.
- The incident shall be responded as per the response time matrix (refer Appendix-B)

6.2 Incident Handling and Response

- Once a potential security incident is reported, it should be logged in the incident tracker (see: Security incidents)
- It should be analyzed to understand the nature of the incident for proper remediation.
- Enough information or evidence shall be collected about the incident so the security team can prioritize the next steps in handling the incident, which is normally containment.
- The incident shall be prioritized as per Appendix -B to get an initial impression of the nature and scope of the incident.
- CISO can also notify the security team who may assist with the initial analysis of the incident. Other appropriate personnel may be notified at this point as well, like relevant IT support staff or a supervisor or department head.
- All details relating to the incident, cause for the incident, actions implemented will be captured in the incident tracker. An incident report will be prepared if required.
- On confirmation of a security incident, containment shall be initiated. The suitable containment shall be done to address the security incident.
- Suitable corrective action is identified and implemented to ensure that the incident shall not recur.
- If any user is found to have breached security policy, they shall be subject to disciplinary action as per the HR process.
- Any violation of the policy by a temporary worker, contractor or supplier shall result in the termination of their contract or assignment.
- After the incident resolution it shall be ensured that the system is restored to normal condition and incident tracker is updated.
- The incident tracker or report shall be updated with the lessons learnt and final report shall be sent to CISO.
- The CISO closely monitor the actions taken on the incident and their closure along with the process owner.

6.3 Monitoring

- An incident log shall be maintained
- The incident log shall be used to identify the trends or outbreaks that require changes to security controls and policies to reduce the future occurrences of incidents.

6.4 Event Identification and Logging

- All the events that could result in the potential loss of data, breaches of confidentiality, unauthorized access or changes to systems shall be reported immediately to the Security officer before taking any actions. (Refer Appendix- A for type of events)
- An event logs / report shall be created and maintained.
- All event logs , Administrator logs are protected from unauthorised access

6.5 Event Response

- Where required, a suitable action shall be identified and initiated in consultation with the Security Team.
- The action shall be completed as per the target date.
- On completion of the action, event report shall be closed.
- Where action is not completed by the date agreed, the situation shall be reviewed and revised actions recorded, taking into account the security risks. A short-term fix shall be identified and implemented until permanent solution is implemented.
- The event reports are analyzed to detect trends and to learn from such events and feedback shall be provided during management review meeting.

7 Escalation

- Where the actions needs assistance from the top management, the same shall be escalated to the CISO for necessary actions
- The decisions of Security Board is recorded in the event report and actions shall be implemented.

8 Clock Synchronization

- Information systems clocks shall be synchronized to a single reference time source.

9 COLLECTION OF EVIDENCE

9.1 Information in paper documents

- The originals to be securely kept with the CISO and he / she will record the details of who, where, when the document was found and the witness details.
- It should be ensured that original documents are not tampered

9.2 Information on computer media

- The mirror image or copies for any removable media, information on hard disks or in memory should be taken to ensure availability.
- The log of the actions relating to copying process are captured and witnessed by two persons.
- It is also to be ensured that the original media and the log should be securely kept un- touched.
- If media can't be taken out a mirror image or copy of the same needs to be kept.

9.3 General

- It is ensured that any forensics work should be done only on the copies of the evidential material
- The integrity of all evidential material should be protected.
- The tools and people used for copying needs to be logged.
- If there is a necessity of involvement of Lawyers / Police the same to be contacted immediately for taking/collecting evidence as required by the law by coordinating with CISO.
- The retention of evidence shall be as per the legal requirement.
- All the evidence to be kept in secured place which has access only to CISO and Security team.
- The lessons learnt shall be documented in the incident tracker for reference by the other stakeholders.

10 VERIFICATION

- Internal Audits
- Incidents discussed in MRM

11 MEASUREMENTS

Number of Incidents reported in the period (year / quarter etc…)

12 RECORDS

- Email
- Incident Report
- Security Incident tracker

13 EXIT CRITERIA

- All Incidents are closed.
- All Events are closed

14 REFERENCES

- Risk management Procedure
- HR Procedure

15 ISO 27001:2013 Standard ISO CLAUSE/CONTROL REFERENCE

ISO 27001:2013 Clause / Control Number	Clause / Control Name
A 16	ation Security Incident Management
A 16.1	ement of information security incidents and improvements Security
A 16.1.1	sibilities & Procedures
2	ing Information Security Events
A 16.1.3	ing Information Security Event & Weaknesses
4	ment of and decision on information security events
5	se to information security incidents
6	g From Information Security Incidents
7	ion of Evidence
A12.4.1	Event logging
A12.4.2	Protection of log information
A12.4.3	Administrator and operator logs
A 12.4.4	Clock synchronization

16 Abbreviations

	nformation Security Officer
	ation Security Management
	s
	plicable
Creative Force	Creative Force

17 Appendix

17.1 Appendix A

Examples of security event and incidents types are:

- Information system failures and loss of service
- Malicious code
- Denial of service
- Errors resulting from incomplete or inaccurate business data
- Breaches of confidentiality and integrity
- Misuse of information system.
- The transfer of sensitive or confidential information to those who are not entitled to receive that information

17.2 Appendix B

17.2.1 Incident Response Time Matrix

Incident Severity	Characteristics (one or more condition present determines the severity)	Response Time	Person responsible	Who to Notify	Post-Incident Report Required
High	1. Significant adverse impact on a large number of systems and/or people 2. Potential large financial risk or legal liability to the company 3. Threatens confidential data 4. Adversely impacts a critical system or service 5. Significant and immediate threat to human safety 6. High probability of propagating to a large number of other systems on or off site and causing significant disruption	*Immediate*	*CISO*	*ISM Security team*	*Yes*
Medium	1. Adversely impacts a moderate number of systems and/or people 2. Adversely impacts a non-critical system or service 3. Adversely impacts a departmental scale system or service 4. Disrupts a building or departmental/functional network 5. Moderate risk of propagating and causing further disruption	*8 hours*	*CISO*	*ISM Security team*	*Yes*
Low	1. Adversely impacts a very small number of non-critical individual systems, services, or people 2. Disrupts a very small number of network devices or segments 3. Little risk of propagation and further disruption	*One day*	*CISO*	*ISM Security team*	*No*
Not Applicable	Used for suspicious activities which upon investigation are determined not to be an IT security incident?				

17.2.2 Examples of possible incidents under above types:

- **Malicious Incident**
    - Computer infected by a virus or other malware, (for example spyware or adware)
    - Finding data that has been changed by an unauthorized person
    - Receiving and forwarding chain letters – Including virus warnings, scam
    - Warnings and other emails which encourage the recipient to forward onto others.
    - Social engineering - Unknown people asking for information which could gain them access to the organization’s data (e.g. a password or details of a third-party).
    - Unauthorized disclosure of sensitive or confidential information electronically, in paper form or verbally.
    - Falsification of records, Inappropriate destruction of records
    - Damage or interruption to the organization’s equipment or services caused deliberately e.g. computer vandalism
    - Connecting third party equipment to the organization’s network
    - Unauthorized Information access or use
    - Giving sensitive or confidential information to someone who should not have access to it - verbally, in writing or electronically
    - Printing or copying sensitive or confidential information and not storing it correctly or confidentially
- **Access Violation**
    - Disclosure of logins to unauthorized people
    - Writing down your password and leaving it on display or somewhere easy to find
    - Accessing systems using someone else's authorization e.g. someone else's user id and password
    - Inappropriately sharing security devices such as access tokens
    - Other compromise of user identity e.g. access to network or specific system by unauthorized person
    - Allowing unauthorized physical access to secure premises e.g. server room, scanning facility.
- **Environmental**
    - Loss of integrity of the data within systems and transferred between systems
    - Damage caused by natural disasters e.g. fire, burst pipes, lighting etc
    - Deterioration of paper records
    - Deterioration of backup tapes
    - Introduction of unauthorized or untested software
    - Information leakage due to software errors
- **Inappropriate use**
    - Accessing inappropriate material on the internet

    - Sending inappropriate emails
    - Use of unapproved or unlicensed software on the organization’s equipment
    - Misuse of facilities, e.g. phoning premium line numbers.

- **Theft / loss Incident**
    - Theft / loss of data – written or electronically held
    - Theft / loss of any of the organization’s equipment including computers,
    - Monitors, mobile phones, Memory sticks, CDs, DVDs, etc…
- **Accidental Incident**
    - Sending an email containing sensitive or confidential information to 'all stAFf' by mistake
    - Receiving unsolicited mail of an offensive nature, e.g. containing pornographic,
    - Receiving unsolicited mail which requires you to enter personal data.
- **Mis-keying**
    - Receiving unauthorized information
    - Sending sensitive or confidential information to wrong recipient.
- **Operational**
    - Loss of service
    - System malfunction