INCIDENT MANAGEMENT POLICY AND PROCEDURE

JANUARY 2020
v.20200110

Incident Management Policy and Procedure

Policy Statement
CorpU will ensure that it reacts appropriately to any actual or suspected incidents relating to information systems and information within the custody of CorpU.

Purpose
The aim of this policy is to ensure that CorpU reacts appropriately to any actual or suspected security incidents relating to information systems and data.

Scope
This document applies to all employees and contracted third parties who use CorpU IT facilities and equipment, or have access to, or custody of, customer information or CorpU information.

All users must understand and adopt use of this policy and are responsible for ensuring the safety and security of CorpU's systems and the information that they use or manipulate.

All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

Definition
This policy needs to be applied as soon as information systems or data are suspected to be or are actually affected by an adverse event which is likely to lead to a security incident.

The definition of an "information management security incident" ('Information Security Incident' in the remainder of this policy and procedure) is an adverse event that has caused or has the potential to cause damage to an organization's assets, reputation and / or personnel. Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

An Information Security Incident includes, but is not restricted to, the following:

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorized access to data or information storage or a computer system.
- Changes to information or data or system hardware, firmware, or software characteristics without the CorpU's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorized use of a system for the processing or storage of data by any person.

Examples of some of the more common forms of Information Security Incidents have been provided in Appendix 1.

Risks
CorpU recognizes that there are risks associated with users accessing and handling information in order to conduct official CorpU business.

This policy aims to mitigate the following risks:

- To reduce the impact of information security breaches by ensuring incidents are followed up correctly.
- To help identify areas for improvement to decrease the risk and impact of future incidents.

Non-compliance with this policy could have a significant effect on the efficient operation of the business and may result in financial loss and an inability to provide necessary services to our customers.

Procedure for Incident Handling
Events and weaknesses need to be reported at the earliest possible stage as they need to be assessed by an Information Security Officer or other process owner. The advisor enables the technology group to identify when a series of events or weaknesses have escalated to become an incident. It is vital for the technology department to gain as much information as possible from the business users to identify if an incident is occurring.

For full details of the procedure for incident handling please refer to Appendix 2.

Policy Compliance
If any user is found to have breached this policy, they may be subject to CorpU's disciplinary procedure. If a criminal offense is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from a Human Resources representative or your supervisor.

Policy Governance
The following table identifies who within CorpU is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- Responsible: the person(s) responsible for developing and implementing the policy.
- Accountable: the person who has ultimate accountability and authority for the policy.
- Consulted: the person(s) or groups to be consulted prior to final policy implementation or amendment.
- Informed: the person(s) or groups to be informed after policy implementation or amendment.

Responsible	The Information Security Officer or process owner
Accountable	The VP of Technology
Consulted	The Information Security Officer and senior management
Informed	All employees and contracted third parties within the scope of this policy

Review and Revision
This policy, and all related appendices, will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the Information Security Officer.

Key Messages
- All staff should report any incidents or suspected incidents immediately by following the incident reporting procedure below.
- We can maintain your anonymity when reporting an incident if you wish.
- If you are unsure of anything in this policy, you should ask for advice from the Human Resources department.

Appendix 1: Examples of Information Security Incidents
Examples of the most common Information Security Incidents are listed below. It should be noted that this list is not exhaustive.

Malicious

- Giving information to someone who should not have access to it - verbally, in writing or electronically.
- Computer infected by a Virus or other malware.
- Sending a sensitive e-mail to 'all staff' by mistake.
- Receiving unsolicited mail of an offensive nature.
- Receiving unsolicited mail which requires you to enter personal data.
- 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.
- Unknown people asking for information that could gain them access to business or customer data (e.g. a password or details of a third party).

Misuse

- Use of unapproved or unlicensed software on CorpU equipment.
- Accessing a computer database using someone else's authorization (e.g. someone else's user id and password).
- Writing down your password and leaving it on display / somewhere easy to find.
- Printing or copying confidential information and not storing it correctly or confidentially.

Theft/Loss

- Theft / loss of a hard copy file.
- Theft / loss of any CorpU computer equipment.
- Theft / loss of any personal computer equipment or mobile devices containing business or customer information

Appendix 2: Procedure for Incident Handling
Reporting Information Security Events or Weaknesses
The following sections detail how users and IT Support Staff must report information security events or weaknesses.

Reporting Information Security Events for all Employees
Security events, for example a virus infection, could quickly spread and cause data loss across the organization. All users must understand and be able to identify that any unexpected or unusual behavior on the workstation could potentially be a software malfunction. If an event is detected users must:

- Note the symptoms and any error messages on screen.
- Disconnect the workstation from the network if an infection is suspected (with assistance from IT Support Staff).
- Not use any removable media (for example USB memory sticks) that may also have been infected.

All suspected security events should be reported immediately to the Information Security Officer.

If the Information Security event is in relation to paper or hard copy information, for example personal information files that may have been stolen from a filing cabinet, this must be reported to Senior Management and either the Data Protection Officer or VP, Technology for the impact to be assessed.

The Information Services Officer will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information must be supplied:

- Contact name and number of people reporting the incident.
- The type of data, information or equipment involved.
- Whether the loss of the data puts any person or other data at risk.
- Location of the incident.
- Description of any equipment affected.
- Date and time the security incident occurred.
- Location of data or equipment affected.
- Type and circumstances of the incident.

Reporting Information Security Weaknesses for all Employees
Security weaknesses, for example a software malfunction, must be reported through the same process as security events. Users must not attempt to prove a security weakness as such an action may be considered to be misuse.

Weaknesses reported to application and service providers by employees must also be reported internally to Information Services. The service provider's response must be monitored and the effectiveness of its action to repair the weakness must be recorded by Information Services.

Reporting Information Security Events for IT Support Staff
Information security events and weaknesses must be reported to a nominated central point of contact within Information Services as quickly as possible and the incident response and escalation procedure must be followed.

Security events can include:

- Uncontrolled system changes.
- Access violations – e.g. password sharing.
- Breaches of physical security.
- Noncompliance with policies.
- Systems being hacked or manipulated.

Security weaknesses can include:

- Inadequate firewall or antivirus protection.
- System malfunctions or overloads.
- Malfunctions of software applications.
- Human errors.

The reporting procedure must be quick and have redundancy built in. All events must be reported to at least two nominated people within Information Services who must both be required to take appropriate action. The reporting procedure must set out the steps that are to be taken and the time frames that must be met.

An escalation procedure must be incorporated into the response process so that users and support staff are aware who else to report the event to if there is not an appropriate response within a defined period.

Incidents must be reported to the Business Continuity Management teams should the incident become service affecting.

Management of Information Security Incidents and Improvements
A consistent approach to dealing with all security events must be maintained across the business. The events must be analyzed, and the Security Advisor must be consulted to establish when security events become escalated to an incident. The incident response procedure must be a seamless continuation of the event reporting process and must include contingency plans to advise the business on continuing operation during the incident.

All incidents should be reported to the Information Security Officer.

Collection of Evidence
If an incident may require information to be collected for an investigation strict rules must be adhered to. The collection of evidence for a potential investigation must be approached with care. The security office as well as Human resources must be contacted immediately for guidance and strict processes must be followed for the collection of forensic evidence. If in doubt about a situation, for example concerning computer misuse, contact the Information Security Officer for advice.

Responsibilities and Procedures
Management responsibilities and appropriate procedures must be established to ensure an effective response against security events. The security advisor from Information Services must decide when events are classified as an incident and determine the most appropriate response.

An incident management process must be created and include details of:

- Identification of the incident, analysis to ascertain its cause and vulnerabilities it exploited.
- Limiting or restricting further impact of the incident.
- Tactics for containing the incident.
- Corrective action to repair and prevent reoccurrence.
- Communication across the interested parties to the those affected.

The process must also include a section referring to the collection of any evidence that might be required for analysis as forensic evidence. The specialist procedure for preserving evidence must be carefully followed.

The actions required to recover from the security incident must be under formal control. Only identified and authorized staff should have access to the affected systems during the incident and all of the remedial actions should be documented in as much detail as possible.

The officer responsible for an incident should risk assess the incident based on the Risk Impact Matrix (please refer to Appendix 3). If the impact is deemed to be high or medium this should be reported immediately to the Information Security Officer.

Learning from Information Security Incidents
To learn from incidents and improve the response process incidents must be recorded and a Post Incident Review conducted. The following details must be retained:

- Types of incidents.
- Volumes of incidents and malfunctions.
- Costs incurred during the incidents.

The information must be collated and reviewed on a regular basis by Information Services and any patterns or trends identified. Any changes to the process made as a result of the Post Incident Review must be formally noted.

Appendix 3: Risk Impact Matrix
To decide on the potential or actual impact of an information security incident, the impact matrix below should be used.

Type of Impact	Reputational Media and Customer Damages	Contractual Losses	Failure to meet Legal Obligations	Financial Loss / Commercial Confidentiality Loss	Disruption to Activities	Personal Privacy Infringement
Low	None	None	None	None	None	None
Low	Contained internally within the business / Unfavorable customer response	Minor contractual problems / minimal SLA failures	Civil lawsuit / small fine - less than $10k	Less than $100k	Minor disruption to service activities that can be recovered	Personal details revealed or compromised
Medium	Unfavorable local media interest / Unfavorable council member response	Significant client dissatisfaction. Major SLA failures. Failure to attract new business	Less than $100k Damages and fine	$100k-$500k	Disruption to service that can be recovered with an intermediate level of difficulty. One back up not backing up for 2 or more days	Personal details revealed or compromised internally within authority. Harm mental or physical to one members of staff or public
High	Sustained local media coverage, extending to national media coverage in the short term	Failure to retain contract(s) at the point of renewal	Greater than $100k damages and fine	$500k-$1m	Major disruption to service which is very difficult to recover from. Two or more systems not being backed up for two or more days	Severe embarrassment to individual(s)
High	Sustained unfavorable national media coverage	Service or product outsourced through Government intervention	Client contract(s) cancelled	Over $1m damages and/or fines	More than $1m	Detrimental effect on personal & professional life OR large-scale compromise affecting many people. Harm mental or physical to two or more members of staff or public

Online
www.corpu.com

About Corp/U
Corp/U grows leaders, who grow companies which make a difference.

For More Information
To learn more about Corp/U, contact sales@corpu.com.

Product Overview
www.corpu.com/technology

Privacy Policy
https://www.corpu.com/privacy-policy

Terms of Service
https://www.corpu.com/terms-of-service

Contact Corp/U
www.corpu.com/contact

Client Support
support@corpu.com