1.0 PURPOSE

This policy addresses the actions required for responding to an information security incident. This policy is intended to improve the chances of quickly containing damage and speeding an efficient IT service recovery. Unauthorized access to the company's data systems is a crime.

2.0 SCOPE

The policy applies to all corporate IT systems to include network devices, telephones, computers, and any devices that store corporate information. It applies to all users of the organization's network, whether internal or third-party partner, using any device that has access to the corporate network.

3.0 POLICY

Everyone, employees and temporary workers, is responsible for reporting suspected information security violations to the service desk immediately. The service desk will assist the information security team in determining the severity of the breach. Incidents involving the compromise of company confidential data will be referred to the company CEO. No public disclosures about any security incident may be made without the company CEO's approval.

The difficult part is containing the damage and halting the intrusion while still maintaining availability to other IT systems. The initial reaction may be to cut the external network connection but such as interruption to customers and company employees only adds to the damage. It all depends on the situation.

Speed is important to contain the damage. Incidents to report include:

- Loss of a company computing device that stores data, such as a memory stick, a CD containing company data, a notebook PC, tablet, cell phone, etc.
- Unauthorized access to company confidential data.
- Computers infected with malware such as a worm, virus, Trojan Horse, ransomware or botnet.
- Reconnaissance activities such as scanning the network for security vulnerabilities.
- Denial of Service attack.
- Web site defacement.
- Theft of documents containing confidential information.
- An attempted social engineering attack.

3.1 Roles and Responsibilities

- The Information Security Manager is responsible for:
  - Managing the containment and recovery from an information security incident.
  - Creating, implementing, testing, and maintaining an incident response plan.
  - Identifying the tools and forms necessary to contain and recover from a security breach.
  - Identifying the incident response team members (and their backup support) and ensuring they are properly trained in incident response.
  - Declaring when the incident response team will be summoned.
  - Working with the response team during an incident and providing information status to the IT Director.
- The Information Security team members are responsible for:
  - Promptly responding when called to address an incident.
  - Studying the incident response plan and where appropriate, suggest improvements to improve effectiveness and efficiency.
  - Participating in plan exercises and the lessons learned in discussions.
- The IT Director is responsible for:
  - Communicating the security incident status to company executives. The IT director is the single point of contact between the security team and the executives.
  - Ensuring that issues discovered during plan tests and audits are promptly resolved.
  - Ensuring the incident response plan is tested regularly.
- The IT Service Desk is responsible for:
  - Gathering the information reported to them about a security breach and promptly passing it on to the information security manager. They are not to judge its validity.
  - Being available during their normal 24 by 7 coverage time to receive end user and customer incident reports.

3.2 Types of Company Confidential Data

The company has different types of information that it is legally mandated to keep confidential in all jurisdictions where it collects, processes or stores data. In addition, trade secrets must be protected or they lose their legal safeguard.

- Data:
  - Legal compliance—any data elements with company financial records
  - PII and PHI must be protected from disclosure such as payroll and personnel records

- Company proprietary information—Data that provides a competitive advantage—customer contact lists, results of expensive research, designs of upcoming models, how much you pay for materials, etc.
- Company trade secrets—special formulations and processes

- Legal compliance for other IT areas, such as access and data change controls on financial systems.
- Management directives—IT areas that management stipulates must also be protected even if not in the previous categories.

PII uniquely identifies an individual. Sometimes several pieces must be combined to do so. Determined thieves can combine data stolen from your system with information readily available on social media to overcome security questions. PII in this company is found in Human Resource department and payroll records. There is also PII for companies in the sales records.

- Name
- Social Security Number
- Driver's license or state ID
- Credit card numbers
- Financial account numbers
- Home address
- Email address
- Date of Birth
- Phone number
- Birthplace
- Biometric Identifiers (such as retinal scans, finger prints, voice prints)
- Health insurance account number

3.4 Report an Incident

All security incidents, whether witnessed or suspected, must be immediately reported to the IT Service Desk. The service desk will gather and pass on the information to the information security team.

3.5 Incident Response

A. Validating that a data breach has occurred. Examine the initial information and available logs to confirm that a breach has occurred. Intrusion detection systems are known to generate ''false positive'' events. The problem may be an erratically running device or a software problem. If the incident is confirmed, then the plan is activated.
B. The information security manager summons the response team and begins an incident-tracking log.
C. Open the communications bridge so that anyone off-site can join in.
D. Assess the situation:
   - If the incident is ongoing, contain the damage. If it is not ongoing, assess the extent of the damage.

- Based in the extent of the damage, inform management (usually the IT Director or Information Security Manager) of the situation. That person becomes the single point of contact between the response team and company executives.
- The Information Security Manager decides whether or not to recommend calling in a Cybersecurity Investigator to oversee the collection of evidence for a potential prosecution.

E. Contain the hardware involved by leaving it on but disconnected from the network.
F. Identifying the type of information disclosed and estimating the method of disclosure (internal/external disclosure, malicious attack, or accidental).
G. Identifying all affected systems, data, and devices.
H. Check all systems for potential break-ins and the introduction of ''back doors.''
I. Preserve evidence when possible using backups, photos of screen images, data hash values, and hardware for use in the investigation.
J. Making copies of all log files from affected systems.
K. Record actions taken for addressing and/or mitigating the cause(s) of the data breach.

3.6 Post Incident Review

After the incident has been contained, the Information Security Manager will conduct a lessons discussion with all team members involved. The goal is to clarify what occurred and how well the incident response plan performed. Attendees are encouraged to indicate places to improve the efficiency and effectiveness of the plan and how it was applied.

A formal report on the incident must be submitted to the IT Director within one week of its resolution. The report is to indicate, in as non-technical terms as practical, what occurred and how it was resolved. It must also contain a technical assessment of damage done to the company.

4.0 EXCEPTIONS TO THIS POLICY

Any exceptions to this policy must be approved in advance by the company's IT information security manager.

5.0 POTENTIAL PENALTIES FOR POLICY VIOLATION

- Company employees who violate this policy may be suspended from work without pay for a period of time or discharged.
- Temporary employees will be discharged back to their agencies.
- Unauthorized access to the company's IT systems and data is a crime. Depending on the nature of the incident, the potential damage to the company or compromise of confidential data, the details of the incident may be submitted to law enforcement for prosecution.

6.0 REVISION HISTORY

Date	Revision #	Description of Change
04/01/18	1.0	Initial creation.

7.0 INQUIRIES

Direct inquiries about this policy to:

George Jenkins, CIO
Email: gjenkins@company.com