2020

INFORMATION SECURITY POLICY

VERSION 2

SEPTEMBER 2020

INFORMATION SECURITY POLICY

1. SUMMARY

Information is the livelihood of our business.

Without it, employees cannot work, customers cannot interact with the business, bills cannot be paid, and profits cannot be earned.

Any given technological environment is useless if its main purpose for existence, the processing and sharing of information, is threatened or eliminated.

With that in mind, a sound policy on how to secure business information is essential for smooth company operations and ensuring a successful future.

2. PURPOSE

This policy provides guidelines to safeguard company information, reduce business and legal risk, and protect company investments and reputation. It covers data. Its adjunct policy, the Network Security Policy, covers the systems and devices that transport and store data.

3. SCOPE

All part-time and full-time employees, contractors, consultants, interns, volunteers, and visitors are covered by this policy. It also applies to all software that is owned/developed by or licensed to the company, as well as workstations, servers, and other devices that are used to create, access, or modify company data.

4. EXCEPTIONS

There are no exceptions to this policy.

5. POLICY DETAILS

To safeguard data, it is necessary to establish what constitutes acceptable/unacceptable use of systems and identify responsibilities for employees, IT staff, and supervisors/managers.

6. ACCEPTABLE USE OF SYSTEMS

Employees using company equipment (or their own equipment for company purposes) are representing the company whether during or after company hours. Employees are responsible for ensuring that this equipment is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Accessing file shares or databases to work on company-owned material that the employee needs to perform their job duties.
- Using web browsers to obtain business information from commercial websites.
- Using email for business communication.
- Accessing information on a company-owned mobile device.
- Printing confidential documents for a staff meeting.

7. UNNACEPTABLE USE OF SYSTEMS

Employees must not use company equipment for purposes that are illegal, unethical, harmful to the company, or non-productive, as this places the Company at risk. Examples of unacceptable use are:

- Playing games, engaging in online gambling, or accessing offensive/inappropriate material.
- Broadcasting non-work-related email to internal or external recipients.
- Conducting personal business using company resources.
- Transmitting any content that is offensive, harassing, or fraudulent.
- Accessing information employees are not authorized to access or do not need to perform their job duties.
- Accessing or sharing pirated software or material.
- Attempting to disrupt or hack other systems (internally or externally) or produce malicious results, such as damaging systems, stealing/removing data, and planting viruses.

8. EMPLOYEE RESPONSIBILITIES

An employee who uses the company workstations or systems to conduct business operations must:

- Ensure that all equipment used is for business/professional purposes.
- Access only information that is needed to perform their jobs or assist others in doing so as part of the valid scope of their duties.
- Be responsible for the content of all data, including text, audio, and images they share internally or externally.
- All communications should have the employee's name attached.
- Be responsible for all actions/transactions performed with their accounts.
- Never leave workstations or devices used for company business unattended. Use passwords and screen locks on company-owned systems or devices, or those that have been approved for access to company data.

- Log out when leaving a workstation for an extended period.
- Never share private passwords with those who are not authorized to have them, or leave passwords in an accessible place (such as on a post-it note).
- Passwords must be changed immediately if it is suspected that they may have become known to others.
- Store all shared passwords (such as for departmental accounts) in a centralized and encrypted password database, such as Password Safe or KeePass.
- The main password for these databases must also be kept private and provided only to authorized individuals.
- Change passwords per company policy (eg, every 90 days).
- Not copy or transfer copyrighted materials without permission.
- Not copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner.
- Know and abide by all applicable company policies dealing with security and confidentiality of company records.
- Avoid transmission of private or confidential information.
- If it is necessary to transmit this data, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use.
- Share and store private or confidential information by adhering to security restrictions (eg, via encrypted transmission or encrypted media).
- For instance, they must not keep private or confidential information on unsecured media or employee-owned or unsecured devices, such as flash drives or laptops, or employee-owned cloud storage applications.
- Download files only from known good sources for business purposes.
- All systems handling these files must have updated anti-malware programs that must not be disabled or tampered with.
- Run a virus scan on any executable file(s) received through the internet.
- If a virus is found (either during a scan or via a check by anti-malware software, the employee should power off the system and immediately contact the IT department to notify them of the situation, then take no further action until instructed otherwise.
- Never knowingly access, put, or use pirated software, viruses, or other malware on company systems.
- Install only software that is company owned and/or authorized for use by the IT department.

- Never access, insert, or connect to company systems any disks, USB drives, or other storage media of unknown origin.
- Not take portable equipment such as laptop computers out of the business unless it has been assigned to them for use or they have the informed consent of their department manager or the IT department.
- Informed consent means that the appropriate authorizing individual knows what equipment is leaving, what data is on it, and what it will be used for.
- Exercise care to safeguard the valuable electronic equipment assigned to them.
- Employees who neglect this duty may be accountable for any loss or damage that may result.
- Never use or access company resources remotely via unsecured wireless networks (hotels, coffee shops, etc).
- Never permit unauthorized individuals (even family members) to access company-owned systems or devices.
- Hand in all company-issued systems or devices upon termination of employment.
- Submit any employee-owned systems or devices that have accessed company resources to the IT department for inspection upon termination or when the system/device no longer requires this access.
- Notify the IT department of all passwords, as well as the whereabouts of any confidential data and any other details that should be transferred to others upon termination of employment.

9. I.T. CONSULTANT'S RESPONSIBILITY

The IT department must:

- Perform all equipment installations, disconnections, modifications, and relocations.
- Work with departmental managers to establish a standard set of access policies for different employees based on their roles and responsibilities.
- Administer access controls to all company computer systems and ensure that employees are granted only the access needed to do their jobs.
- Process adds, deletions, and changes of user accounts, systems, and devices.
- Install and maintain appropriate anti-malware software on all systems where applicable, including workstations, servers, and mobile devices.
- Respond to all malware attacks, destroy any detected malware, and document each incident.
- Respond to all security breaches, whether suspected or confirmed, as well as assist and comply with any investigations, whether internal or external.

- Maintain records of software licenses owned by the company.
- Periodically (at least quarterly) scan company computers and systems for vulnerabilities and security threats and verify that only authorized software is installed.
- Implement access and security logging on all critical systems and not tamper with or remove these logs.
- Enact security systems and controls to ensure compliance to this policy (blocking the use of unauthorized USB devices, using data-loss-prevention software to prevent the transmission of credit card data, etc).
- Conduct security sweeps to ensure compliance with this policy; confirm that employees secure their devices, lock their workstations, do not store illegal material on workstations, devices, or company systems, do not transmit confidential material via insecure means, and other controls .
- Monitor backups and cloud/remote storage to ensure that confidential information is secured.
- Inspect all employee-owned devices that have accessed company resources to be sure that no confidential data exists on these devices once the employee is terminated or the access is no longer required.
- Keep abreast of the latest security threats, engage in ongoing security training, and develop plans and processes for the organization so it can continue to operate in a secure fashion.
- Provide appropriate support and guidance to help employees fulfil their responsibilities under this directive.
- Conduct training for employees to keep them aware of current and upcoming security threats or factors.
- Adhere to any regulations that may apply to the business, such as PCI or HIPAA.
- Develop and maintain written standards and procedures necessary to ensure the implementation of and compliance with these policy directives.
- Recognize that security is a journey—not a destination.
- It is never a concept that is “finished” or “good enough”.

10. MANAGER AND SUPERVISOR RESPONSIBILITIES

Managers and supervisors should notify the IT Consultants promptly whenever an employee leaves the company or transfers to another department so that their access can be revoked.

- Involuntary terminations must be reported concurrent with the termination.

- Managers and supervisors must also: Ensure that all appropriate personnel are aware of and comply with this policy.
- Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.
- Assist the IT consultants via any means necessary to ensure that this policy is adhered to and comply with any analyses or investigations as needed.
- Notify the IT Consultants on a monthly basis of new associates, associate transfers, and employee terminations.
- Assist the IT Consultants via any means necessary to ensure that this policy is adhered to and comply with any analyses or investigations as needed.

11. MONITORING

The IT department is responsible for the implementation of and adherence to this policy.

- All policy changes must be implemented and approved by the administration and any related documentation should be updated accordingly.
- Employees must note that all data created, sent, or retrieved (whether locally or over the internet) is the property of the company and may be regarded as public information.
- This data may be defined as (but not limited to) email messages, Office documents, database entries, voicemails, text messages, images, instant messages, and physical documentation.
- The company reserves the right to access the contents of this data if the company believes, in its sole judgment, that it has a business need to do so.
- All data can be disclosed to law enforcement.

12. VIOLATION & PENALTIES

Violations of this policy must be immediately reported to any involved managers and the IT department.

Violating the policy or any of its tenets could result in disciplinary action by the company depending upon the type and severity of the violation, whether it causes any liability or loss to the company, and/or the presence of any repeated violation(s).

13. ACKNOWLEDGMENT OF INFORMATION SECURITY POLICY

This form is used to acknowledge receipt of and compliance with the company's Information Security.

POLICY PROCEDURE
Complete the following steps:

- 1 - Read the Information Security Policy.
- 2 - Sign and date in the spaces provided.
- 3 - Return a copy of this signed document to the Human Resources department.

SIGNATURE
Your signature attests that you agree to the following terms:

- I have received and read a copy of the Information Security Policy and I understand and agree to the same.
- I understand the organization may monitor the implementation of and adherence to this policy to review the results.
- I understand that violations of the Information Security Policy could result in termination of my employment and legal action against me.

_____
Signature

_____
Name

_____
Date

_____
Department / Location

Disclaimer : This policy is not a substitute for legal advice. If you have legal questions related to this policy, please consult with your legal practitioner.