IMAGEWORLD

SECURITY PLAN

IMAGEWORLD DIGITAL PRINTING, INC.

2023

UNIVERSITY OF SOUTHEASTERN PHILIPPINES
1978

PREPARED BY:

LESTAT LOUIS ARIOLA
GABRIEL ENOBIO
CHESTER JOHN ESTRELLA
JOHN ALDREICH ROSALES

Table of Contents

INTRODUCTION

BACKGROUND OF THE COMPANY

ImageWorld Digital Printing, Inc. is a printing company, and is a part of the commercial industry. It was founded and established on January 31, 2009, and is still running with Mr. Bartolome M. Hernandez III as the current president. They offer products and services like yearbook printings, newsletters, magazines, brochures, flyers, and many more. ImageWorld Digital Printing, Inc. can be considered as one of the huge printing companies of the City of Davao and are producing their products with state-of-the-art equipment, machineries – digital and conventional – and the latest software applications operated and maneuvered by their expert pool of human resource.

The company, like every starting business, is struggling in their early years, but eventually found a smooth path after their 3rd year in the business. By providing quality prints from their yearbooks, which is their pride of a product, ImageWorld has provided a lot of huge schools and universities in the City of Davao: University of Southeastern Philippines, Holy Cross of Davao College, Davao Doctors College, and more.

The company's organizational structure is a functional organizational structure. As the hierarchy of positions from the Board of Directors comes down, each department of the company is divided and shown in the structure, and has one person on the helm of each department with vice-superiors under it. From the President, Mr. Bartolome Hernandez III, and the Board of Directors, he is the one that oversees all departments: Sales & Marketing, Production, Finance Administration and Human Resource. And there are supervisors following Mr. Bart's lead of each department.

PURPOSE

The purpose of this Information Security Plan is to safeguard ImageWorld's assets, which may include sensitive data, software, hardware and other vital resources against potential threats or cyber attacks. This plan shows our constructed policies, procedures and controls when it comes to maintaining the confidentiality, integrity, and availability of ImageWorld's information assets, while ensuring applicable laws and regulations will be followed.

The objectives of this plan are to:

1. Identify and assess the risks associated with ImageWorld's assets and liabilities, as we implement the appropriate solutions to specific risks.

2. Secure that all employees and contractors who have access to ImageWorld’s assets will be aware and comply with this information security plan’s policies and guidelines.
3. Provide a framework for responses to security incidents and disaster recoveries that will affect ImageWorld’s assets.
4. Constantly monitor and evaluate ImageWorld’s information security condition to identify potential threats and vulnerabilities and address them.

With the implementation of this information security plan, we intend to protect ImageWorld from reputational damage, financial loss and legal liabilities that could possibly result from a security breach. This plan will be viewed regularly and updated as time goes, to ensure its effectiveness and relevance to evolving business needs and the landscape of security.

SCOPE

This information security plan is applied to all the managers, employees, staff, temporary workers, and guests who have access to valuable information, and especially to all important assets owned, controlled, or processed by ImageWorld, including but not limited to customer information, financial data, employee records, and confidential business information.

Aspects to Consider

Asset identification - Identify all the assets that need to be protected, including hardware, software, and sensitive data.

Confidentiality - It is important that confidential information can only be accessed by authorized employees.

Risk assessment - Assess the potential threats and vulnerabilities that could impact the confidentiality, integrity, and availability of your assets.

Security controls - Implement technical, administrative, and physical controls to enforce your security policies and procedures, such as firewalls, intrusion detection and prevention systems.

Employee training - Ensure that all employees are aware of your security policies and procedures, and train them on how to identify and respond to security threats.

Computer Security - Check if the hardwares and softwares are working properly and require a security update.

Monitoring and testing - Regularly monitor and test your security controls to ensure they are effective and up-to-date.

Continuous improvement - Continuously improve your security plan by reviewing and updating it on a regular basis to address new risks and emerging threats.

Backup and recovery - Develop and implement a backup and recovery plan to ensure that critical data and systems can be restored in case of a disaster or system failure.

Wireless Connectivity (Wi-Fi) Policy

ImageWorld

Introduction:

The purpose of this policy is to provide guidelines for the secure and appropriate use of wireless connectivity/Wi-Fi within ImageWorld. This policy aims to protect the company's confidential information, prevent unauthorized access, and ensure the availability and integrity of wireless networks.

Objective:

The objective of this policy is to:

- Ensure the security of wireless connectivity/Wi-Fi within the organization building and during working hours.
- Protect confidential information, intellectual property, and personal data from unauthorized access, modification, disclosure, and destruction.
- Prevent security incidents and data breaches caused by misuse, abuse, or negligence of wireless connectivity/Wi-Fi.
- Comply with relevant laws, regulations, and industry standards for information security.
- Foster a culture of awareness, responsibility, and accountability for information security among employees, contractors, and third parties.
- Continuously monitor, evaluate, and improve the effectiveness of the wireless connectivity/Wi-Fi security controls and risk management process.

Policy Number:	001	**Version No.**	1
Policy Name:	Wi-Fi Policy	**Date Drafted/Created**	Apr 23, 2023

Overview:

Wireless networks are an integral part of modern business operations. However, they also pose a significant risk to the security of an organization's information. Wireless networks are susceptible to unauthorized access, eavesdropping, and interference. As such, it is essential that ImageWorld implements proper security measures to ensure the confidentiality, integrity, and availability of its wireless networks.

Policy Statement:

The policy aims to safeguard against unauthorized access, misuse, and data breaches by implementing appropriate security controls and measures. This policy also seeks to protect the organization's assets and information, as well as the privacy of its employees and customers, by promoting responsible and secure wireless connectivity practices.

Scope:

This policy applies to all employees, contractors, and visitors who use the wireless network provided by ImageWorld during working hours and while on the organization's premises. It covers all devices that connect to the wireless network, including laptops, smartphones, tablets, and other wireless-enabled devices. This policy governs the use of wireless connectivity within ImageWorld's facilities and premises, and it is designed to safeguard the confidentiality, integrity, and availability of ImageWorld's information assets and IT infrastructure. This policy extends to all locations where ImageWorld's wireless network is accessible.

This policy does not cover the use of personal mobile devices that are not connected to ImageWorld's wireless network, or the use of wired network connections. Additionally, this policy does not apply to visitors who have been granted access to the wireless network for a limited time period, such as guests or vendors. It is the responsibility of the authorized employee or contractor to ensure that guests and vendors are aware of and adhere to this policy. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract, as well as legal action where applicable.

Roles and Responsibilities:

1. **IT Department:** The IT department is responsible for setting up and managing the wireless network infrastructure. This includes configuring access points, managing network settings, and ensuring that the network is secure and protected from external threats.

2. **Employees:** All employees are responsible for using the wireless network in a secure and responsible manner. This includes not sharing passwords, not accessing unauthorized websites or applications, and reporting any suspicious activity on the network.

3. **Management:** Management is responsible for ensuring that all employees are aware of this policy and are following the established guidelines for wireless

network use. They are also responsible for providing the necessary resources to the IT department to ensure that the wireless network infrastructure is properly maintained and updated.

4. **Third-Party Contractors/Guest:** Third-party contractors who require access to the wireless network must adhere to this policy and follow the guidelines set forth by the IT department. The IT department will provide contractors with the necessary access credentials and monitor their activity on the network.

Definition:

1. **Wireless Connectivity/Wi-Fi:** refers to the wireless network infrastructure that allows users to connect to the Internet or other network resources without the need for physical cables.

2. **Access Points (APs):** are hardware devices that enable wireless communication between devices and the network.

3. **Network Administrator:** the individual responsible for managing and maintaining the organization's wireless network infrastructure, including security protocols and access controls.

4. **Employees:** individuals who are authorized to use the organization's wireless network infrastructure for work-related purposes.

5. **Third-Party/Guests:** individuals who are not employees of the organization but are granted temporary access to the wireless network infrastructure for a specific purpose, such as attending a meeting or conference.

6. **Security Controls:** technical or administrative measures put in place to mitigate the risks associated with wireless connectivity, including authentication, encryption, and network segmentation.

Policy Detail:

1. **Authorized Personnel Only:** Only authorized personnel may connect to ImageWorld's wireless networks. Employees and contractors may use their own devices if needed, but it must be authorized by the IT department.

   1.1. All wireless connectivity and Wi-Fi within the organization's premises are strictly for use by authorized personnel only.

1.2. Employees who require wireless connectivity access for work purposes must request authorization from the IT department.

1.3. Authorization requests must be approved by the IT department and the employee's immediate supervisor.

1.4. The IT department will maintain a list of authorized personnel and their corresponding access privileges.

1.5. Authorized personnel must use their own unique login credentials to access the organization's wireless connectivity.

1.6. Sharing of login credentials is strictly prohibited.

1.7. Employees must not disclose their login credentials to anyone.

1.8. The IT department will monitor the wireless network and take necessary actions for any unauthorized access or breach of security.

1.9. Violation of this policy may result in disciplinary action, up to and including termination of employment.

2. **Strong Passwords/Authentication:** Wireless networks must be secured with strong passwords or other authentication methods.

2.1. Passwords must contain a minimum of 12 characters and include a combination of upper and lowercase letters, numbers, and special characters.

2.2. Employees must not use the same password across multiple accounts and systems.

2.3. Multi-factor authentication should be implemented where possible.

2.4. Default passwords on any devices or systems must be changed immediately upon installation.

2.5. Passwords must not be written down or shared with anyone.

2.6. Any suspicion of a password compromise must be immediately reported to the IT department.

2.7. System access must be revoked immediately for any terminated or suspended employees.

3. **Encryption:** Wireless networks must be configured to use encryption, such as WPA2, to protect against attacks. Employees and contractors must not attempt to disable or circumvent encryption on wireless networks.

3.1. All wireless communications within the organization must be encrypted using the latest security protocols available.

3.2. All data transmitted over the network must be encrypted using AES-256 or higher encryption standards.

3.3. Encryption keys must be stored securely and separately from the data they protect.

3.4. Passwords used to access encrypted data must be strong and meet the organization's password policy standards.

3.5. Mobile devices that access the organization's wireless network must have encryption enabled for all data in transit and at rest.

3.6. The use of unencrypted personal devices to access the organization's wireless network is prohibited.

3.7. The IT Department will conduct regular reviews of its encryption policies to ensure that they are up to date with the latest standards and best practices in the industry.

4. **Public Wi-Fi Networks:** The use of public Wi-Fi networks for business purposes is strictly prohibited. Employees and contractors must use ImageWorld's wireless networks for business purposes only.

4.1. Employees are prohibited from accessing public Wi-Fi networks using company-issued devices.

4.2. Employees must avoid accessing any suspicious websites or downloading any unauthorized applications while using public Wi-Fi networks.

4.3. Employees must not use public Wi-Fi networks for work-related tasks unless they are using a secure virtual private network (VPN) connection.

4.4. Employees must avoid accessing sensitive company information or personal accounts while using public Wi-Fi networks.

4.5. Employees must ensure that their devices are configured to not automatically connect to public Wi-Fi networks without explicit consent.

4.6. Employees must avoid using public Wi-Fi networks in areas where people can see the screen or keyboard, such as in cafes, airports, or other public places.

4.7. Employees must disconnect from public Wi-Fi networks immediately after completing their tasks.

5. **Unauthorized Access:** Unauthorized access to ImageWorld's wireless networks is strictly prohibited. Employees and contractors must not attempt to access wireless networks that they are not authorized to use.

5.1. Any employee found to have intentionally gained unauthorized access to the company's wireless network or any other information system will be subject to disciplinary action, up to and including termination of employment.

5.2. Any employee found to have inadvertently compromised the company's wireless network or any other information system due to negligence or failure to comply with the company's information security policy will be subject to disciplinary action, which may include verbal or written warnings, suspension, or termination of employment.

5.3. Any third-party individual found to have gained unauthorized access to the company's wireless network or any other information system will be reported to the appropriate authorities and may be subject to legal action.

5.4. Any employee found to have shared their login credentials with unauthorized personnel or failed to report any suspected unauthorized access will be subject to disciplinary action, up to and including termination of employment.

5.5. All employees are expected to report any suspected unauthorized access or security breach immediately to their supervisor or the IT department.

5.6. All incidents of unauthorized access or security breach will be thoroughly investigated, and appropriate actions will be taken to prevent similar incidents from occurring in the future.

6. **Personal Wireless Devices:** The use of personal wireless devices on ImageWorld's wireless networks is not allowed. Employees and contractors must use company-issued devices that have been authorized by the IT department.

6.1. Employees are not allowed to connect their personal wireless devices to ImageWorld's network, unless the device has been authorized by the IT department and meets the security requirements set by the organization.

6.2. Personal wireless devices must be protected with strong passwords and encryption to ensure confidentiality and prevent unauthorized access to sensitive information.

6.3. Employees must not use personal wireless devices to access or store confidential information, unless the information has been authorized to be accessed or stored on personal devices by the relevant department head.

6.4. In case of lost or stolen personal wireless devices, employees must immediately report to the IT department to prevent unauthorized access to ImageWorld's network and sensitive information.

6.5. Employees must also follow the organization's guidelines and standards regarding the use of personal wireless devices for work-related purposes outside of the organization's building and network.

7. **Security Patches and Anti-Virus Software:** All wireless devices, including laptops and mobile phones, must be updated with the latest security patches and anti-virus software to prevent malware infections and other security vulnerabilities.

7.1. All computers and devices connected to the organization's Wi-Fi network must have up-to-date anti-virus software and security patches installed.

7.2. All anti-virus software and security patches must be obtained from reputable sources and regularly updated.

7.3. All employees must immediately report any security patches or anti-virus software warnings or notifications to the IT department.

7.4. Employees must not attempt to disable, modify or remove any security patches or anti-virus software without permission from the IT department.

7.5. Any device found to be infected with a virus or malware will be immediately disconnected from the organization's Wi-Fi network and quarantined.

7.6. All devices must undergo a virus scan before connecting to the organization's Wi-Fi network. If a device is found to be infected with a virus or malware, it will not be allowed to connect until it is fully cleaned.

7.7. The IT department will conduct regular checks to ensure all devices connected to the Wi-Fi network have up-to-date anti-virus software and security patches installed. Any device found to be non-compliant will be disconnected from the Wi-Fi network until it is updated.

Risk Assessment:

The risk assessment process will be conducted by the IT department with the involvement of relevant stakeholders across the organization. The process will involve the identification of potential vulnerabilities and threats associated with wireless connectivity and Wi-Fi usage, as well as the evaluation of existing controls to determine their effectiveness in addressing identified risks.

The risk assessment process will be conducted on a regular basis to ensure that any changes in the organization's IT infrastructure or business operations are taken into consideration. The results of the risk assessment will be used to inform the development and implementation of appropriate security measures to mitigate identified risks.

All employees are responsible for reporting any security incidents or concerns related to wireless connectivity and Wi-Fi usage to the IT department. The IT department will investigate reported incidents, and if necessary, conduct additional risk assessments to determine the impact and likelihood of a breach.

Procedures:

IT Department: The IT department is responsible for ensuring that all wireless access points are properly configured, secured, and maintained. They must also ensure that all staff members are aware of the policy and trained on how to use the wireless network securely. In addition, the IT department should conduct regular risk assessments to identify vulnerabilities in the wireless network and take appropriate measures to address them.

Employees: All employees must comply with the policy and report any suspicious or unauthorized activities immediately to the IT department. Employees are responsible for securing their own wireless devices and ensuring that they only connect to authorized networks. They should also use strong passwords and two-factor authentication to access the wireless network.

Visitors: Visitors must be supervised by an authorized employee while using the wireless network. They must also comply with the policy and connect only to authorized networks. Visitors are not allowed to connect any unauthorized devices to the network, and they should not share their login credentials with anyone.

Reporting: All suspected violations of this policy must be reported immediately to the IT department. The IT department will investigate all reported violations and take appropriate action. Employees and visitors who report suspected violations in good faith will be protected from retaliation.

Penalties: Violations of this policy may result in disciplinary action, up to and including termination of employment, and/or legal action if necessary. The severity of the penalty will depend on the nature and severity of the violation. Employees who violate the policy will be subject to disciplinary action, while visitors who violate the policy may be denied access to the network.

E-mail Policy
ImageWorld

Introduction:

This policy will provide best practices and clear guidelines to help ImageWorld mitigate the risks and threats concerning their company Email accounts. By implementing this policy, the company of ImageWorld will have a secure Email environment that protects their confidential, sensitive, and important data/information.

Objective:

The objectives of this policy are:

- **Protect sensitive information:** Ensure that all company and customer data transmitted through email is secured and protected from unauthorized access, theft, or theft.
- **Prevent security breaches:** Minimize the risk of security breaches caused by phishing scams, malware, or other cyber threats that can compromise our network and systems.
- **Ensure compliance:** Comply with all relevant regulatory requirements related to email security.
- **Promote best practices:** Encourage all employees of ImageWorld to follow best practices for email security, including strong password management, encryption, and appropriate use of company email.
- **Establish accountability:** Clearly define roles and responsibilities for email security and establish consequences for employees who violate the policy.

Policy Number:	002	**Version No.**	1
Policy Name:	E-mail Policy	**Date Drafted/Created**	Apr 24, 2023

Overview:

The email policy for the security plan that we are developing aims to establish guidelines and best practices for the safe and secure use of email within ImageWorld. This policy will cover topics such as password management, encryption, phishing prevention, and appropriate use of company email. It will also outline the roles and responsibilities for email security and establish consequences for employees who violate the policy.

Policy Statement:

The email policy for security plan aims to establish clear guidelines and best practices for the safe and secure use of email within ImageWorld. Our policy statement reflects our commitment to protect sensitive information, preventing security breaches, ensuring compliance, establishing accountability, and promoting best practices for email security.

Scope:

The email policy for the security plan includes all employees that are assigned to a task that requires them to use a computer. The policy applies to all email communication sent or received on company-owned devices or through company-owned email accounts. This policy applies to all types of email communication, including internal and external emails, as well as attachments and links contained within those emails.

This policy does not cover personal email accounts or personal devices used to access company email accounts. However, employees are reminded to be cautious when forwarding or sharing company information via personal email or devices, as it can still pose a risk to ImageWorld security.

Additionally, this policy is subject to periodic review and updates to ensure that it remains effective in protecting the company’s data and complying with regulatory requirements. Any changes to the policy will be communicated to all employees in a timely manner.

Roles and Responsibilities:

1. **Management:** The management team is responsible for developing and implementing the email policy for the security plan. They will ensure that the policy aligns with the company's overall security strategy and regulatory requirements.

2. **IT Department:** The IT department will be responsible for enforcing the email policy for the security plan. They will ensure that all company-owned devices and email accounts are properly configured and secured according to the policy.

3. **Employees:** All employees are responsible for following the email policy for the security plan. They are required to adhere to best practices for email security, use company email only for business purposes, and report any suspected security breaches or incidents to the IT department.

4. **Human Resources:** The human resources department will be responsible for enforcing the policy in case of violation. They will investigate and take appropriate disciplinary action against employees who violate the policy.

Definitions:

1. **Email:** is a form of digital communication that allows users to send and receive messages and attachments through the internet or other computer networks.

2. **Email accounts:** are digital accounts that allow users to send, receive, and manage email messages. Each email account has a unique email address that consists of a username and a domain name, such as username@example.com

3. **Security Breach:** refers to an incident where an unauthorized individual or entity gains access to sensitive or confidential information without proper authorization. A security breach can occur due to various reasons, such as malware or hacking attacks, human error, or physical theft.

4. **Encryption:** is the process of converting plain, readable data into a coded format using mathematical algorithms to protect its confidentiality and integrity during transmission or storage.

5. **Phishing:** is a type of cyber attack in which an attacker attempts to trick individuals into divulging sensitive information such as usernames, passwords, or credit card details by posing as a legitimate entity in an electronic communication such as an email, text message or social media message.

6. **Malware:** refers to any software intentionally designed to cause harm to computer systems, networks, or devices. Malware can come in different forms, including viruses, worms, Trojans, and ransomware, and can cause various damages, such as data theft, system damage, and financial loss.

7. **Cyber Threats:** are any malicious activities or attacks on computer systems, networks, or devices that aim to exploit vulnerabilities and cause harm.

Policy Detail:

1. **Authorized use:** Employees are permitted to use ImageWorld email for official business purposes only. Personal or private use of the email system is prohibited, except in cases where prior approval has been granted by the management.

   1.1. Employees are authorized to use the ImageWorld email system solely for conducting official business.

   1.2. Personal use of the ImageWorld email system is strictly prohibited unless prior approval has been granted by the management.

   1.3. Personal use should not consume a significant amount of the company's resources or cause any disruption to the workplace.

   1.4. The use of ImageWorld email accounts for personal communication must not interfere with the employee's job responsibilities or impact the productivity of the organization.

   1.5. Employees who have been granted approval for personal use must comply with the ImageWorld's email policy and use the email system in accordance with the ethical and legal standards of the organization.

2. **Confidentiality:** Employees are expected to use good judgment when sending emails and must ensure that confidential information is not disclosed. Confidential information includes but is not limited to customer data, financial information, and trade secrets. Employees must encrypt sensitive information and follow the company's data protection policies.

   2.1. Employees are responsible for ensuring the protection of confidential information contained in email messages.

   2.2. Employees must follow the ImageWorld's data protection policies and procedures to safeguard this information.

   2.3. Employees must encrypt any email messages containing sensitive information or confidential data that are sent outside the company network.

   2.4. Employees must exercise caution when opening email attachments as they may contain viruses or malware that can compromise the security of the company's systems.

   2.5. Employees must ensure that email attachments containing confidential information are password-protected and encrypted before being sent.

   2.6. Employees must follow the company's data retention policy and dispose of email messages containing confidential information in a secure manner.

3. **Prohibited Activities:** The use of the ImageWorld email system for illegal or unethical activities is prohibited. This includes but is not limited to the transmission of offensive or discriminatory content, chain letters, or spam. Employees are prohibited from sending or receiving messages that violate the company's code of conduct or legal obligations.

    3.1. Employees are prohibited from sending or receiving email messages containing offensive or discriminatory content, including but not limited to material that is defamatory, harassing, or threatening in nature.
    3.2. Employees are prohibited from sending chain letters or unsolicited email messages, commonly known as spam.
    3.3. Employees must not use email to engage in activities that violate the ImageWorlds's code of conduct or ethical standards.
    3.4. Employees must comply with all legal obligations when using the ImageWorld email system.
    3.5. Employees must not use the ImageWorld email system for personal gain or financial benefit. This includes but is not limited to soliciting business, promoting personal ventures, or engaging in any activities that could compromise the ImageWorld's reputation or interests.

4. **Password Policy:** The supervisor/s are required to create a strong password for the employee's accounts which is difficult to guess and change regularly. Passwords must be at least eight characters long and include a combination of upper and lower case letters, numbers, and special characters. Employees must not share their passwords with others and must log out of their email accounts when not in use.

    4.1. Supervisor/s must create strong passwords that are at least 8 characters long and include a combination of upper and lower case letters, numbers, and symbols.
    4.2. Passwords should be changed regularly, at least 90 days, to prevent unauthorized access to the ImageWorld's systems.
    4.3. Passwords should not be reused, and employees should not write them down or share them with anyone.
    4.4. Two-factor authentication should be used whenever possible to provide an additional layer of security to the ImageWorld's email system.
    4.5. The IT department should conduct regular password audits to ensure that employees are following the password policy.
    4.6. They should also use software tools to detect weak passwords or passwords that have been compromised in data breaches and require employees to update them immediately.

5. **Penalties:** An email policy is an essential aspect of any security plan, as email is a common vector for cyber attacks. To ensure that employees follow email security best practices, it's important to establish clear penalties for policy violations. Here's an example of a penalty policy for email security:

   5.1. **First Offense:** Verbal warning - The employee will be informed of the violation and reminded of ImageWorld's email policy. A written record of the violation and the warning will be kept.
   5.2. **Second Offense:** Written warning - If the employee violates the email policy again, they will receive a written warning, which will be added to their personnel file. The warning will also specify that a third violation may result in suspension or termination.
   5.3. **Third offense:** Suspension - If the employee violates the email policy for the third time, they will be suspended from work without pay for a specified period. The length of the suspension will depend on the severity of the violation and the employee's past performance.
   5.4. **Fourth offense**: Termination - If the employee violates the email policy for the fourth time, they will be terminated from their employment.

Risk Assessment:

ImageWorld shall conduct regular risk assessments to identify potential security risks related to email accounts. This assessment will be carried out following industry best practices and will focus on identifying and addressing security vulnerabilities that may be exploited by attackers. The risk assessment shall include, but not be limited to, the following:

- **Identify potential risks:** The risk assessment will identify potential risks to email accounts, including but not limited to unauthorized access, phishing attacks, and password cracking.
- **Analyze the likelihood of occurrence**: The risk assessment will evaluate the likelihood of each potential risk occurring.
- **Evaluate the impact of each risk:** The risk assessment will assess the potential impact of each risk, including financial, reputational, and legal consequences.
- **Identify controls to mitigate risks:** Based on the risk assessment, controls will be identified to mitigate identified risks. These controls may include strong password policies, two-factor authentication, and training programs.
- **Monitor and update controls:** ImageWorld will regularly monitor and update the effectiveness of the controls implemented to mitigate risks.

By conducting regular risk assessments and implementing appropriate security controls, ImageWorld can prevent email security defects and vulnerabilities and reduce the risk of data breaches and other security incidents related to email accounts. Additionally, ImageWorld should provide employees with regular training on email security best practices to ensure that they are aware of potential risks and how to mitigate them.

Procedures:

IT Department Supervisor: The IT department supervisor is responsible for creating email accounts for every employee. These accounts should be properly configured and apply the appropriate security measures in setting up the password for each account. The supervisor should regularly change passwords to ensure security for each email account and to avoid the risks of being compromised.

Employees: All employees that are associated with email accounts should comply with the policy and immediately report any suspicious activities that they encounter to the IT department.

Penalties: Inappropriate actions should face the consequences stated above. There should be no excuses to violators who constantly make violations and keep damaging or exposing risks to the company. Termination of employment will be given to those employees who keep receiving a violation.

Hardware Policy

ImageWorld

Introduction:

The hardware used by an organization is critical to the success of its operations. ImageWorld, as a printing company, relies heavily on its hardware infrastructure to provide quality products and services to its clients. This Hardware Policy aims to provide guidance and establish standards for the use and management of all hardware resources owned by ImageWorld.

Objective:

The objective of this policy is to:

- Ensure that all hardware assets are managed in a secure and effective manner.
- Protect company resources and information from unauthorized access, theft, or damage caused by hardware failures or malfunctions.
- Maximize the lifespan of hardware assets through proper maintenance and upgrade procedures.
- Ensure compliance with legal and regulatory requirements regarding hardware asset management.
- Promote the efficient use of hardware assets to minimize unnecessary costs and improve productivity.
- Provide clear guidance and expectations for employees regarding their responsibilities in relation to hardware assets.

Policy Number:	003	**Version No.**	1
Policy Name:	Hardware Policy	**Date Drafted/Created**	Apr 25, 2023

Overview:

Hardware equipment is one of the critical assets in any organization. In ImageWorld, hardware equipment such as computers, laptops, printers, and other peripherals are crucial to the success of our printing services. ImageWorld aims to ensure the security, availability, and integrity of its hardware infrastructure and prevent any unauthorized access, theft, damage, or misuse of its hardware resources. It is important that all employees and contractors of ImageWorld understand and comply with this policy to maintain a secure and reliable hardware environment.

Policy Statement:

ImageWorld is committed to ensuring the proper management, utilization, maintenance, and security of all hardware equipment within the organization. The policy outlines the guidelines and procedures to achieve this objective.

Scope:

This policy applies to all hardware assets owned or leased by ImageWorld, including all hardware equipment used by ImageWorld's employees, contractors, and third-party vendors to access ImageWorld's networks, systems, or data. The policy applies to all hardware devices, including but not limited to, desktop computers, laptops, servers, printers, mobile phones, tablets, and any other devices used for business purposes.

It is the responsibility of all employees and contractors to comply with this policy and ensure that all hardware assets are used appropriately and maintained in a secure and efficient manner. Any violation of this policy may result in disciplinary action up to and including termination of employment or contract.

Roles and Responsibilities:

IT Department: Responsible for implementing this policy and ensuring that all hardware devices are configured in accordance with this policy. Responsible for maintaining hardware devices and ensuring that they are secure, properly functioning, and up-to-date.

Management: Responsible for supporting the implementation of this policy and ensuring that all employees comply with the policy. Responsible for providing the necessary resources and support to the IT department to effectively implement and maintain this policy.

Employees: Responsible for complying with this policy and reporting any hardware-related issues or incidents to the IT department. Responsible for safeguarding the hardware devices assigned to them and using them in a responsible and secure manner.

Third-Parties: Must comply with this policy when accessing or using ImageWorld's hardware devices. Responsible for ensuring that any hardware devices or equipment provided by them are secure and do not pose a threat to ImageWorld's security.

Definitions:

- **Hardware devices:** Refers to all computer equipment, peripherals, and other devices used in the organization, including but not limited to desktop computers, laptops, printers, scanners, servers, storage devices, mobile devices, and other network-connected devices.
- **End-users:** All employees, contractors, or other personnel who have access to the hardware devices owned by ImageWorld.
- **Authorized users:** Refers to all employees, contractors, and third-party vendors who are authorized by ImageWorld to use its hardware devices for business purposes.
- **BYOD:** Bring Your Own Device. This refers to any personal hardware device owned by an employee, contractor, or other personnel that is used for work purposes within the organization.
- **Inventory:** A record of all hardware devices owned by ImageWorld, including their make, model, and serial number.
- **Maintenance:** Any actions taken to keep hardware devices in good working condition, such as updates, repairs, or replacements.
- **Disposal:** The process of securely removing all data and information from a hardware device and disposing of it in an environmentally friendly manner. This can include recycling or donating devices that are still in good condition.

Policy Detail:

1. **Procurement Process:** Acquiring hardware equipment through authorized channels and approved vendors.

   1.1. All hardware equipment purchases must be approved by the IT department and comply with the organization's budget.
   1.2. The procurement process must follow the organization's procurement policies and procedures.
   1.3. The IT department is responsible for ensuring that all hardware purchases meet the necessary technical specifications, security requirements, and compatibility with the organization's existing infrastructure.
   1.4. The IT department will maintain a list of approved hardware vendors and devices.

2. **Inventory Management:** Tracking and managing hardware equipment owned by the organization, including the location, status, and condition of each item.

   2.1. The IT department will maintain an accurate and up-to-date inventory of all hardware equipment, including its location and status.
   2.2. All hardware equipment must be labeled with a unique identification number for inventory tracking purposes.
   2.3. End-users must report any changes to hardware equipment location or status to the IT department promptly.
   2.4. The IT department will conduct periodic physical inventory audits to ensure the accuracy of the inventory records.

3. **Use of Hardware Equipment:** The proper and authorized use of hardware equipment by end-users for work-related activities only.

   3.1. End-users are responsible for the proper use of hardware equipment and must follow the organization's acceptable use policy.
   3.2. End-users must not use hardware equipment for personal purposes or install any unauthorized software.
   3.3. End-users must immediately report any hardware equipment malfunctions or damages to the IT department.

4. **Security of Hardware Equipment**: The protection of hardware equipment from theft, loss, damage, or unauthorized access or use.

   4.1. All hardware equipment must be protected with appropriate physical security measures, such as locks, cables, or alarms.
   4.2. End-users must not leave hardware equipment unattended in public areas or unsecured areas.
   4.3. The IT department will implement appropriate security controls, such as antivirus software, firewalls, and access controls, to protect hardware equipment from security threats.

5. **Maintenance and Repairs**: Maintaining and repairing hardware equipment to ensure its optimal performance, functionality, and security.

   5.1. The IT department is responsible for maintaining and repairing hardware equipment.
   5.2. End-users must report any hardware equipment issues to the IT department immediately.
   5.3. The IT department will establish a regular maintenance schedule for hardware equipment, including firmware and software updates, and perform repairs as necessary.

6. **Third-party Access:** The authorized access to hardware equipment by third-party vendors, contractors, or service providers for maintenance, repairs, or other approved purposes.

   6.1. Any third-party vendors or contractors who require access to the organization's hardware equipment must sign a confidentiality agreement and follow the organization's security policies and procedures.
   6.2. The IT department will ensure that third-party access is granted only on a need-to-know basis and for the minimum necessary period.

7. **Disposal of Hardware Equipment:** The proper and secure disposal of hardware equipment that is no longer needed or functional, in accordance with applicable laws, regulations, and organizational policies.

   7.1. All hardware equipment must be disposed of in a manner that ensures the protection of sensitive data and compliance with local environmental regulations.
   7.2. The IT department will ensure that all hardware equipment is securely wiped of any sensitive data before disposal.
   7.3. The IT department will dispose of hardware equipment following the organization's policies and procedures, including donating or selling equipment in good condition or recycling obsolete equipment.

Risk Assessment:

The responsibility of developing and conducting Risk Assessments lies with the IT department. They will conduct regular assessments to identify potential threats and vulnerabilities, analyze the likelihood and impact of these threats, and implement appropriate measures to mitigate the risks.

Risk assessments should be conducted at least annually or as needed to ensure the security of our hardware devices and data. The results of the risk assessments should be documented and reviewed by the management to ensure that appropriate controls are in place.

Any identified risks that require immediate attention must be reported to the IT department, and appropriate actions must be taken to address these risks. Failure to follow the procedures outlined in this policy may result in disciplinary action.

Procedures:

IT Department: The IT department is responsible for overseeing the implementation of this policy and ensuring that all hardware equipment is properly maintained and secure. To achieve this, the IT department shall carry out the following procedures:

- Regularly conduct risk assessments to identify potential threats and vulnerabilities to the hardware equipment.
- Implement appropriate security measures, such as access controls, firewalls, antivirus software, and encryption, to protect the hardware equipment.
- Provide regular training to end-users on the proper use and handling of hardware equipment.
- Monitor the use of hardware equipment to ensure that it is being used appropriately and in accordance with this policy.
- Ensure that all hardware equipment is properly maintained and repaired as necessary.

Employees: All employees are responsible for ensuring the security of the hardware equipment they use. To achieve this, employees shall carry out the following procedures:

- Use hardware equipment only for its intended purpose and in accordance with this policy and protect hardware equipment from damage, theft, or loss by securing it when not in use.
- Report any loss, theft, or damage of hardware equipment to the IT department immediately.
- Immediately report any suspicious activity or potential security breaches involving hardware equipment to the IT department.

Third-Parties: Third-parties who are granted access to hardware equipment shall comply with the provisions of this policy. To achieve this, third-parties shall carry out the following procedures:

- Sign a non-disclosure agreement before being granted access to hardware equipment.
- Use hardware equipment only for the intended purpose.
- Return hardware equipment immediately after use.
- Report any loss, theft, or damage of hardware equipment to the IT department immediately.

Management: Management shall ensure that all employees and third-parties are aware of this policy and are following the procedures outlined in it. To achieve this, management shall carry out the following procedures:

- Provide regular training to employees and third-parties on this policy and its procedures and ensure that this policy is reviewed and updated regularly.
- Provide the necessary resources and support to the IT department to implement this policy effectively.

Software Policy
ImageWorld

Introduction:

The software used by an organization is just as essential and critical to the success of its operations as its other part, hardware. ImageWorld Digital Printing, Inc. utilizes up-to-date software that caters to the design and structure of the expected products of the clients, where yearbooks are the prominent product that this company produces. This Software Policy aims to provide quality guidelines and standards on the software usage that is happening inside the company to maintain quality production of the products.

Objective:

The objective of this policy is to:

- Secure a strong and well-managed handling foundation of all software used by the company and all its production processes.
- Protect company assets and resources that pass through the software used in production.
- Ensure that all software used are credible, legal and safe.
- Secure that only authorized staff and personnel can access certain software that are critical to the production of the products by the company.

Policy Number:	004	**Version No.**	1
Policy Name:	Software Policy	**Date Drafted/Created**	Apr 25, 2023

Overview:

Considering the primary source of income of products that the company has, maintaining the software usage and its access is essential and key towards the productivity and continuity of the company's business operations. Whether it be from photo editing, layout designs, up to printing, the software is as important as the hardware components and parts of the operations. ImageWorld's vision and goal is to provide quality prints of yearbooks and other printed materials towards their clients, so by having the best software usage while also maintaining and assuring the software used in production is pivotal towards the company's success. Putting a policy in place is a good step towards the company's vision and goal. The policy would lead all the employees into following a set standard and maintain the quality of service that the company provides.

Policy Statement:

ImageWorld recognizes the importance of software as a crucial component of its business operations and success. To ensure that software aligns with the company's goals, is secure, and licensed, we have implemented a software policy.

Scope:

This policy applies to all software assets owned and legally handled by ImageWorld, including all software used for all the processes in production and all the company's employees, contractors, and all third parties concerned and included.

It is the responsibility of all employees and contractors to comply with this policy to ensure that there would be no possible data breaches and malware attacks due to software misuse and abuse. Any violation of this policy may result in disciplinary action up to and including termination of employment of contract.

Roles and Responsibilities:

IT Department: Responsible for implementing this policy and ensuring that all software programs are properly installed, properly configured and in accordance with the policy. Responsible for maintaining and handling all software programs used by the company.

Management: Responsible for supporting the implementation of the policy and ensuring that all employees comply with the policy. Responsible for monitoring all the employees with proper software usage and no illegal use happening inside the company's premises.

Employees: Responsible for complying with this policy and reporting any software-related issues or incidents to the IT department or to the Management. Responsible for properly using all software programs in accordance with the policy.

Third-Parties: Must comply with this policy when using and utilizing all the software programs that the company uses. Responsible for ensuring that all actions concerned are followed in accordance with the contracts in place and the policy provided to ensure that they do not disrupt the company's business continuity in case any threats or attacks occur in the software department that the company uses.

Definitions:

Software Programs: Refers to all software programs that are installed, configured in accordance with the company’s procedures and processes in production of all products and services offered. It includes editing software, printing software, and other software that can and may be connected to the hardware components of the production department of the company.
End-users: All employees from all departments inside the company who have access and always use the software programs during office hours.
Authorized users: Refers to users that are part of the IT Management department of the company, where they have access and authority to use certain and specific software for the production of the products of the company.
Update and Maintenance: The process of updating, maintaining and making sure that the software programs used by the company are running properly, smoothly and are up-to-date.

Policy Detail:

1. **Procurement Process:** Acquiring software applications through authorized channels and approved vendors.

   1.1. All software purchases must be approved by the IT department and comply with the organization's budget.
   1.2. The procurement process must follow the organization's procurement policies and procedures.
   1.3. The IT department is responsible for ensuring that all software purchases meet the necessary technical specifications, security requirements, and compatibility with the organization's existing infrastructure.

2. **Use of Software Programs:** The proper and authorized use of software applications by end-users for work-related activities only.

   2.1. End-users are responsible for the proper use of hardware equipment and must follow the organization's acceptable use policy.
   2.2. End-users must not use software applications for personal purposes or install any unauthorized application.
   2.3. End-users must immediately report any software system malfunctions or damages to the IT department.

3. **Security of Software Programs:**: The protection of the system from cyber attack, loss, damage, or unauthorized access or use.

3.1. All software applications must be protected with appropriate security measures, such as passwords, encryptions and two-factor authenticators.

3.2. End-users must not leave software apps unattended in public areas or unsecured areas.

3.3. The IT department will implement appropriate security controls, such as antivirus software, firewalls, and access controls.

4. **Maintenance and Repairs**: Maintaining and repairing software state to ensure its optimal performance, functionality, and security.

4.1. The IT department is responsible for maintaining optimal performance and repairing software issues.

4.2. End-users must report any software issues to the IT department immediately.

4.3. The IT department will establish a regular maintenance schedule for firmware and software updates, and perform repairs as necessary.

5. **Third-party Access:** The authorized access to software applications by third-party vendors, contractors, or service providers for maintenance, repairs, or other approved purposes.

5.1. Any third-party vendors or contractors who require access to the organization's softwares must sign a confidentiality agreement and follow the organization's security policies and procedures.

5.2. The IT department will ensure that third-party access is granted only on a need-to-know basis and for the minimum necessary period.

6. **Deletion of Software Programs:** The proper and secure disposal of software files that is no longer needed or functional, in accordance with applicable laws, regulations, and organizational policies.

6.1. All software files must be disposed of in a manner that ensures the protection of sensitive data and compliance with local environmental regulations.

6.2. The IT department will ensure that all software files are securely wiped of any sensitive data before disposal.

6.3. The IT department will dispose of software files following the organization's policies and procedures.

Risk Assessment:

A software policy security plan is essential for protecting ImageWorld's sensitive data and ensuring the reliability and availability of its software applications. A risk assessment section is a crucial part of such a plan, as it identifies potential security risks and provides a framework for mitigating them.

There are two main types of software security risks: internal and external. Internal risks can arise from within an organization, such as unauthorized access or data theft by employees. External risks can be caused by hackers, malware infections, or other external threats.

Unauthorized access is a significant internal risk that can lead to data theft, data manipulation, and other malicious activities. To mitigate this risk, access controls such as password policies, two-factor authentication, and regular access audits should be implemented.
Malware is another significant risk that can compromise the integrity of software and cause data loss or system crashes. To prevent malware infections, anti-malware software should be installed on all systems, and employees should be trained on safe browsing habits and instructed to avoid downloading software from untrusted sources.

Data breaches are another major risk that organizations must address, especially in the ImageWorld Inc. which handles a lot of personal data of students from different schools. These can occur when sensitive data is accessed or stolen by unauthorized individuals, resulting in legal and financial liabilities, loss of customer trust, and damage to ImageWorld's reputation. To mitigate this risk, data encryption should be enforced using industry-standard encryption algorithms, both in transit and at rest.

By implementing these measures, ImageWorld can effectively mitigate the risks associated with software security and ensure the confidentiality, integrity, and availability of sensitive data. Regular security assessments and audits will help maintain the effectiveness of these measures and ensure the continued protection of the organization's software and data. It is crucial to educate employees on the importance of software security and their roles in maintaining a secure environment. All employees should receive regular security awareness training, phishing simulations, and other relevant education to help them identify and prevent social engineering attacks.

Procedures:

IT Department: The IT department is responsible for overseeing the implementation of this policy and ensuring that all software systems are properly maintained and secure. To achieve this, the IT department shall carry out the following procedures:

- Regularly conduct risk assessments to identify potential threats and vulnerabilities to the software programs.
- Implement appropriate security measures, such as access controls, firewalls, antivirus software, and encryption.
- Provide regular training to end-users on the proper use and handling of software programs.
- Monitor the use of software programs to ensure that it is being used appropriately and in accordance with this policy.
- Ensure that the software system is properly maintained and repaired as necessary.

Employees: All employees are responsible for ensuring the security of the software system they use. To achieve this, employees shall carry out the following procedures:

- Use software programs only for its intended purpose and in accordance with this policy and protect the system from cyber attacks, malwares, or loss by securing it when not in use.
- Report any problem or issue of the software system to the IT department immediately.
- Immediately report any suspicious activity or potential security breaches to the IT department.

Third-Parties: Third-parties who are granted access to hardware equipment shall comply with the provisions of this policy. To achieve this, third-parties shall carry out the following procedures:

- Sign a non-disclosure agreement before being granted access to software programs.
- Use software programs only for the intended purpose.
- Report any problem or issue of the software system to the IT department immediately.

Management: Management shall ensure that all employees and third-parties are aware of this policy and are following the procedures outlined in it. To achieve this, management shall carry out the following procedures:

- Provide regular training to employees and third-parties on this policy and its procedures and ensure that this policy is reviewed and updated regularly.
- Provide the necessary resources and support to the IT department to implement this policy effectively.

Information Security Plan

IMAGEWORLD

DIGITAL PRINTING, INC.

An Information Security Plan
Prepared by:

Ariola, Lestat Louis C.
Enobio, Gabriel P.
Estrella, Chester John O.
Rosales, John Aldreich C.

Bachelor of Science in Information Technology

April 2023