**7-1 Final Project: Gap Analysis Document**

**Guysell Dixson**

**Information System, Southern New Hampshire**

**IT 355: Security Principles 22EW4**

**Ryan McAurthur**

**April 17, 2022**

# TABLE of CONTENT

***Executive Summary pg.3***

***Organizational Background pg.3***

***Scope pg.3***

***Security Posture pg.3***

***Seven Domain of IT Infrastructure pg.4-5***

***Findings pg.5-7***

***Standard Policy Documentation List pg.7-11***

***Policy Overview pg.12-14***

***Data Security Guideline pg.15.16***

***Implementation Plan and Sample pg.17-18***

***Life Cycle Diagram pg.19***

***References pg.20***

**Executive Summary**

Wilbur’s Widget Company (WWC) is a mid-size company with 82 employees. The company suffers from out-of-date practices and lack of current technologies. This report has been created to show the vulnerable state that WWC is currently in and how to shift the company’s poor security posture, to a line with the industry’s current best practices and regulations. WWC is running on outdated operating systems and lack of updated policies to protect the company, shareholders, and customers. After running reports, doing surveys, and observing daily operations, the following reports will reveal the risks, threats and vulnerabilities facing WWC as well as recommendations to strengthen WWC’s security stance.

**Organizational Background**

Wilbur’s Widget Company is a high- level tech company that currently employ 82 employees. They range from sales, manufacturing, inventory control, research and development, marketing, IT and Human Resource. Wilbur’s Widgets Company is a publicly traded company that is ran by a board of directors and CEOs. Currently this company needs a quality control and quality assurance done. Their policies, procedures and principles all need to be reviewed and brought into alignment with the industry standards for information system security and with International Organization for Standardization.

**Scope**

I will be performing a security analysis to determine Wilbur’s Widgets Company (WWC) security posture. The areas of concerns that will be a focus are WWC’s policies as it pertains to regulation and industry best practice, the status of their hardware and software and network layout. I will also be looking at the risks, threats and vulnerabilities within the IT infrastructure and give recommendations to resolve or mitigate the issues and justify why.

**Security Posture**

Wilbur’s Widget Company is at high risk. Wilbur’s Widget weak security policy, outdated hardware and software and its untrained team members leaves the company open to multiple potential attacks. To start off, as I did a walk through, I noticed confidential work left unsecure on team members desks these documents could easily be stolen or replicated and used for whatever malicious purposes without anyone knowing. I noticed that when team members left their workstations that computer screens were left unlocked, this is another risk that could lead to the network being hacked, or a spyware being uploaded to send all saved documents back to an unknown location. Upon further examination, I have noticed that WWC is running on outdated software. Windows XP SP1 is not compatible with current processors and is not supported by Microsoft. Meaning that there are not up to date viruses and malware protection, there are not patches to protect against new attacks and it does not meet regulation. Seeing that WWC only employs only 7 IT team members and they do not have the ability to train and be proactive, puts WWC at a disadvantage because to have a better security stance this IT team must be both proactive and reactive. The overall security posture is weak and leaves WWC vulnerable and at risk of attacks and legal and financial repercussion.

**Seven Domains of IT Infrastructure**

Wilbur’s Widgets Company faces the same challenges that many other small companies faces when it comes to information security. With a lack of understanding protocols and procedures to remain compliant and within regulations a company can leave themselves open to many risks, vulnerabilities, and threats. The following assessment for Wilbur’s Widgets Company (WWC) will discuss the risks, threats and/or vulnerabilities associated with the seven domains of IT infrastructure.

**Users**: WWC has a small company and the no matter how strong of a security posture any company can develop and implement, the user will be the weakest link. In WWC the lack of any technological knowledge from the board of directors and CEO’s put the company at risk of not taking security seriously. That position on security being modeled, unknowing encourages the frontline team members to be laxed and ill-advised when it comes to protecting passwords, confidential documents, locking their computers, securing documents, and making sure not to expose the company to risks. The user could fall for email phishing, download unknown viruses into the infrastructure and or export information from the company and lose it. The user poses the biggest risk. That is why onboarding, training, and modelling a security culture is important to try to lower this risk.

**Workstation**: As with users, the workstations become an apparent risk at WWC. If the user is untrained and a clean desk/ clear screen policy is not in place, the workstation can be just as easily exploited. The workstation included the physical area as well as laptops, desktops, all smart devices, and paper documents. The risk comes into place when physical and electronic documents are not secure, devices are not locked and protected with passwords and or biometric lock, and Screens are left unattended, or user is not aware of their surroundings. This allows attackers to easily remove information needed to gain access to the system and corrupt or extract information that can cause billions of dollars of damages. To rectify this risk, all workstations should be clear of important documents, passwords should not be written down and in an easily accessible place, when a user is not actively using a screen device, it should be locked and any documents, physical or electronic should be secured locked in a secure place or encrypted to prevent ease of readability.

**LAN**: Local area networks can be a risk due to the physical location or the connections. The threats of LANs are misconfigurations, meaning the layout is wrong or the topography was used. This could cause a drop of communications or worst an opening for a hacker to find their way onto the network. Denial of Service (DoS) could be a threat because if a large amount of traffic is sent over the network this could create a backdoor for hackers to use. Outdated virus database also poses a threat. With WWC lack of security this is likely a major concern. Having an outdated virus/ malware database means that when new viruses and malware comes out the systems has no way to detect and try to quarantine it from the rest of the network. By updating the database will help strengthen WWC security posture.

**WAN**: Wide area network could be at risk for WWC because of a lack of a strong security stance. This creates a situation where there are security gaps and within a WAN could be exploited by a hacker to gain access to the network. This gap again points to the outdated virus and malware protections. Within a WAN it also opens WWC to phishing scams and possible network compromise. WWC should ensure that staff is trained on phishing scams, all security protocol that applies to incoming and outgoing information over external internet be scanned and dealt with in accordance with regulation and procedures.

**LAN-to-WAN**: Local to wide area networks. Is a combination of risk from the local and wide area. WWC risk becomes more substantial when allowing their intranet to communicate with the external internet. If firewalls are not configured properly or a DMZ is not developed to protect their servers, a hacker can easily break through the firewall and gain access causing chaos or even hiding there procuring information without being detected.

**Remote Access**: WWC has been affected by COVID just like the entire world and because of this has resulted in allowing remote access to its servers. The risk that comes from this, besides the lack of IT team members and the lack of tech knowledge from the board and CEOs can result in the hijacking of company computers. WWC needs to implicate a two-factor authentication to safely grant access to remote users. When using a remote access, WWC should consider using a VPN, virtual private network, to create a more secure connection.

**System/Application**: The risk of a system software is that it can become outdated and/or misconfigured. WWC should make sure that all system software is placed on a scheduled maintenance program and is regularly inspected and tested. The risk of application software is that if misconfigured or poorly coded, end users could have access to information or areas of the network that should be restricted to only authorized users. WWC will need to make sure that all applications are overviewed and tested for any security backdoors or to see if privilege can be elevated by users by bypassing administrative authorization.

The above seven domains of IT infrastructures are just a few things that Wilbur’s Widgets Company should be aware of and plan to set controls, protocols, and procedures in pace to handle this risk before they arise and become too overwhelming to mitigate

**Findings**

**Insecure Posture Problem**

Wilbur’s Widgets Company (WWC) suffers from a lack of information security standards and best practices. Upon examining WWC’s network diagram it becomes clearer that there is a lack of structure within information security. The network suffers from a lack of firewalls. Firewalls should be placed between the ISP and the modem, the internet, and the DMZ and if budget permits between the DMZ and the router. These lower risks that a hacker could easily bypass any obstacles and gain instant access to WWC network. These firewalls should also be configured to only have certain ports open due to too many open ports leaves a big window of opportunity to again access the network and perform malicious tasks. By placing the firewall on a QA and QC as well as the Inventory Management policy, this should ensure that the routers, modem, server, and PCs are constantly being checked and patched when new updates come available.

**Risk**

With an insecure network, the ability of a hacker to infiltrate the network and plant spyware, malware or even use social attacks becomes easier and more likely to happen. WWC needs to reconfigure their network and create a star topography with firewalls and DMZs. The LAN to WAN poses a threat to WWC because it opens them up to phishing scams, remote access being exploited and denial of services occurring because of a high traffic on the network. Within that high traffic could be a virus or malware. One solution could be a firewall that is configured to scan and limit the package size along with a well configured switch or router. WWC should implement ISO27001 section 10.6 Network Security Management Policy. This policy will help with managing network security solutions for firewalls and intrusion detection systems.

**Threats**

WWC runs the threat of data breach due to a lack of security protocols not being in place. Without a way to protect the sever network, hackers can elevate privilege and dive deeper into restricted files and gain access to personal identifying information and accounts from marketing and accounting. This could cost WWC millions of dollars and their reputation. By using an inventory management policy, WWC could keep account of data, devices, and hardware. Again, implementing firewalls and switches to direct and filter incoming and outgoing packets could help mitigate these threats.

**User Training**

WWC should train all employees on security policies such as but not limited to, acceptable use policy, clear desk, clean screen policy, email use policy, creation of strong passwords, bring your own device (BYOD) policy, internet use policy and information security practices such as but not limited to, when to report misuse of company property, how to spot a phishing scam, making sure all important documents are secure and not left in plain sight. WWC’s ability to implement these policy and practices will help strengthen their security posture. Getting the board and CEOs to model this new security policies and practices will help reenforce the security culture

Hopefully get everyone to take security seriously.

**Technology Implementation**

As mentioned earlier throughout the assessment, putting firewalls in place on the network will help mitigate unwanted packets from reaching servers and routers. By adding switches into the network, they can scan for viruses and malware to help protect the network from hackers. WWC lack of any type of security measures in place. By implementing hardware that will help with intrusion detection, viruses, and malwares detection, and by using an application software to help configure security, will help WWC add value to their network.

**Security Awareness Training**

WWC should perform security awareness training to keep team members up to date on current security trends, social engineering threats, and remind them on what they can do to help keep WWC safe and secure from unintentional threats, potential threats, and legal violations. By making sure that the suggested policies are put in place, WWC will help strengthen security stances and protect themselves from threats, risks, and vulnerabilities.

Throughout this analysis, risks, threats, vulnerabilities and how to potentially mitigate them. These suggestions are just baseline recommendations for WWC. By making sure that WWC’s team members as well as the board and CEOs are onboard and buy in on the ideas of information security is the best way to ensure a total security perimeter. Only by everyone doing their part can WWC grow in information security posture and protect themselves from legal and reputational ramifications.

**Standard Policy Document List**

Wilbur’s Widgets Company (WWC) has several policies/guidelines and standards in place such as an incident response policy, email policy, acquisition assessment policy, Bluetooth baseline requirement policy, router and switch security policy, password construction guideline and an information logging standard. These are good policies to have in place. In addition to these policies there are several other policies that should be implemented. The following table will layout the proposed policies and how they relate and can impact Wilbur’s Widgets security stance.

|  |  |  |
| --- | --- | --- |
| Proposed Information Security Policies | | |
| Policy | **Reference** | **Justification** |
| Acceptable Use Policy | Based upon NIST 800-53,  ISO/IEC 27002 A.7.1.3 | This policy affects all third-party user, clients, and internal users. This policy will outline the usage of WWC’s company assets such as computers and network system. WWC should implement this policy to control how their assets can be used to deter inappropriate use and or tempering with these assets. |
| Email Acceptable Use Policy | This policy is based upon ISO/IEC FDIS 27002 section 5.1.  NIST 800 800-53  PL-4 | Helps WWC regulate risk from internal and external scams. It establishes the use of the email as a primarily business use only. It also outlines what is acceptable and nonacceptable content such as encrypted email, threaten or offensive emails and political emails |
| Incident Response Policy | This is based on  ISO/IEC 27002 A.13.1, A.13.1.2, & A.12.2.1  NIST SP 800-53 IR-1 | This policy describes the procedures for incident response and the periodic testing of the incident response plan. WWC would benefit from this because it will help to create an incident response plan to ensure that in the case of a breach, they know who is responsible and how to handle it. |
| Internet Access Policy | Based upon NIST SP 800-12 REV 1, this policy is based on least privilege. | Users will have internet access depending on authorization and range of usage needed to perform their respectable job. It will regulate what is an acceptable website, what is an appropriate download and upload based on information being used. It will also help WWC lower potential risks of downloading content containing malware and/or viruses |
| Information Security Policy | This policy is based upon ISO/IEC FDIS 27002 section 5.1. and  NIST 800-53 section SP-1. | This policy will help establish a direction and support for information security in accordance with business requirement and relevant laws and regulations. This will help WWC manage a clear and concise direction on how the organization will handle their IT system. |
| Internal Organization Policy | This based upon ISO/IEC 27002 section 6.1.  NIST SP 800-53 PS-1 | This policy will help manage information security within WWC because the company lacks an internal security structure. |
| Network Security Management | This is based upon ISO/IEC 27002 section A.11.4.5  NIST SP 800-53 AC-4 | Defines secure management of networks, which may span organizational boundaries, requires careful consideration to dataflow, legal implications, monitoring, and protection. WWC has a lack of internal security and by implementing this policy will help strengthen their security posture. |
| Asset Management Inventory Policy | This is based upon ISO/IEC 27002 A.7.1.1  NIST 800-53 CM-8 & PM-5 | Inventories of assets help to ensure that effective asset protection takes place, and may also be required for other business purposes, such as health and safety, insurance or financial (asset management) reasons. The process of compiling an inventory of assets is an important prerequisite of risk management. This policy will help WWC to establish an inventory of all assets and to put into place a maintenance schedule for applying patch management and updating out of date hardware and software |
| Information Security Awareness, Education and Training Policy | This is based upon ISO/IEC FDIS 27002 8.2.2.  NIST SP 800-53 AT-2 | This policy states that a company has obligations to keep all employees trained on the most recent policy change, risk management such as email phishing, and potential risks. WWC will benefits from this policy by creating training programs and by doing this it will help strengthen awareness amongst the employees and create a sense of duty. |
| Clear Desk/Screen Policy | This policy is based upon ISO/IEC FDIS 27002 section 11.3.3  NIST SP 800-53 IA-2 | WWC suffers from document exposure from employees leaving unsecured information on their desk. This policy will help safeguard these document, data, and information by requiring employees to keep their desk organized and computer screens locked when not using it. A clear desk/screen policy reduces the risk of unauthorized access, loss of or damage to information during and after work hours. |
| Termination/ Change Employment Policy | Based on ISO/IEC 27002 8.3.1  NIST SP 800-53 PS-5 | This policy creates awareness that upon departure of service is complete that all credentials, authorizations, and authentications are updated and or removed from the company’s system. WWC needs this policy to help protect against a disgruntle employee after termination. This policy also helps make sure that users have the proper level of authorization. |
| (cont.) Change of Employment Policy | Based on ISO/IEC 27002 A.8.3.2  NIST SP 800-53 PS-4 | Termination or Change of Employment occurs at fast rates. This policy ensures that when level of privilege changes that credential changes as well. This policy creates awareness that upon departure of service is complete that all credentials, authorizations, and authentications are updated and or removed from the company’s system. WWC needs this policy to help protect against a disgruntle employee after termination. This policy also helps make sure that users have the proper level of authorization. |
| Bring Your Own Device Policy (BYOD) add reference | Based on ISO/IEC 27002 A.11.7.1  NIST SP 800-53 AC-19 | This policy will regulate the use of personal devices such as cellphones, tablets, laptop, and portable drives. This policy will outline the usage and consequences for use of these devices. WWC can use this policy to regulate the risks associated with the listed device and go hand in hand with their Bluetooth usage policy. |
| Vulnerability Management Policy | Based on ISO/IEC 27002 A.1.5.2.2  NIST SP 800-53 CA-2 and RA-5 | This policy regulates the frequency and describes the use of internal personnel and/or third-party organizations to provide security reviews and assessments, vulnerability scans, and penetration tests.  WWC would benefit from this policy as it will help keep them aware of any attempts of attack and where patching would be needed. WWC use of this policy would help the 7 IT team member become proactive and reactive as risks and threats are discovered. |
| Risk Management Policy | Based on ISO/IEC 27002 A.14.1.2  NIST SP 800-53 CA-7(1) | This policy describes the risk assessment and risk management process. It will help WWC to establish a routine risk assessment program to monitor their network and be able to make plans on how to handle the situation. |
| Access Control | Based upon ISO/IEC 27002 A.11.2.2  NIST SP 800-53 AC-5 &AC-6 | This policy regulates how an organization ensures that access rights are assigned to enforce segregation of duties and the principle of least privilege. This will ensure that WWC does not give unauthorized access to team members that does not need access higher than job duties. This also ensures that one team member is not in control of two different areas that could contradict or has legal repercussions. |
| Password Management Policy | Based on ISO/IEC 27002 A.11.2.3 & A.11.5.3  NIST SP 800-53 IA-5 | This describes the password controls in place for operating systems and access to critical applications. This policy will help WWC team members create a secure password and how frequently it must be changed. This will also help WWC crate a log of used passwords to keep from having repeat passwords. This will help safeguard from a BOT attack. |
| Change Management Policy | Based on ISO/IEC 27002 A.10.1.3  NIST SP 800-53 CM-5 | Describes the procedures used to migrate changes securely to the production environment. This includes but not limited to the controls in place to ensure that programmers cannot promote their own code, rollback procedures, and recovering from unsuccessful changes and unforeseen events. WWC would benefit from this policy by being able to reboot their system the case that a patch that is installed does not operate correctly. This also gives a fail safe from one person being able to elevate their privilege within the system. |
| Vender Access Policy | Based on ISO/IEC 27002 A.6.2.1  NIST SP 800-53  CA-3 | This policy outlines what assessments that may be performed, before allowing external parties access to WWC’s network, applications, or database. It states what security requirement must be fulfilled before granting a vendor access. |
| Antivirus Policy | Based on ISO/IEC 27002 A.10.4.1  NIST 800-53 SI-3 | This policy defines the requirement that antivirus technology shell be deployed and the type of devices that must be protected by antivirus software in its capability to detect, remove and protect against all known types of malicious software. |

Wilbur’s Widgets Company  
Acceptable use policy

Reference: AUP:001

# Overview

## Purpose and Background

|  |  |
| --- | --- |
|  | This Acceptable Use Policy (AUP) is to establish an appropriate behavior for the use of Wilbur’s Widgets Company’s (WWC) IT System and is designed to protect WWC, employees, customers and other partners from harm caused by misuse of WWC’s IT systems and data. Misuse includes either malicious or accidental actions.  Potential damage includes but is not limited to malware and viruses within the system, legal and financial penalties from data leakage, and lost productivity resulting from a crashed network. As well as loss of WWC reputation amongst customers and partners.  Every “user” accessing Wilbur’s Widgets Company is responsible for the security of WWC’s IT systems which includes, but is not limited to, WWC’s emails, computers, printers, WIFI and data on them. As such every team member must ensure they strictly always follow all guidelines in this policy. Should any “user” be unclear on the policy or how it impacts their role, they should speak with their manager, IT security officer or HR. |

## Definitions

|  |  |
| --- | --- |
|  | “Users” are anyone who has access to any of WWC’s IT system. This includes full-time employees, part-time employees, volunteers, interns, contractors, agencies, consultants, suppliers, customers, and business partners.  “Systems” means all IT equipment that connects to WWC’s network or access WWC’s applications. This includes, but not limited to, laptops, tablets, smartphones known as bring your own device (BYOD) desktop computers, printers, WIFI, software, hardware, portable storage devices all other items commonly understood to be covered by this term. |

## Scope

|  |  |
| --- | --- |
|  | This is a general policy that applies to all Users and all Systems. For some Users and/or some System a more specific policy exists. For other references please refer to associated Resources.  This policy covers only internal use of WWC’s systems and does not cover use of WWC’s products or services by customers or other third parties. |

## Operational Policy

|  |  |
| --- | --- |
|  | * 1. General Use and Ownership      1. WWC intellectual property stored on BYOD, desktops, emails, or servers are sole property of WWC. All WWC’s employees, partners, contractor or third parties must make sure that all data and information are legally and technically secured in compliance with the ISO 27002 6.2 External Parties and ISO 27002 7.2 Information classification.      2. WWC’s team members must report a theft, loss, or unauthorized use of WWC’s data and information.      3. WWC’s users should only access authorized websites when using company’s systems. Each department are responsible for creating guidelines when it comes to acceptable behaviors when using WWC’s Systems.      4. WWC holds the legal right to monitor and audit the systems in compliance with ISO/IEC 27001 6.1 Internal Organization Policy.      5. Internet/Intranet is prohibited from being used to search for pornography, personal usage such as online shopping and media streaming.      6. Social Media is prohibited to use to demeanor or slander the image, name, or public confidence of WWC. HR and Marketing will be allowed to use social media as a marketing tool and to promote events within the company only. Any other reason must be approved by the Information Security Office and Director of HR.      7. External emails will be filtered and/or screened for spamming unless permission is given by the IT director. All confidential/ high priority emails being sent out must be encrypted and all incoming emails will be scanned for viruses and malware. |
|  |  |

## Roles and Responsibilities

|  |  |
| --- | --- |
|  | All WWC’s Users are responsible for adhering to the policies and guidelines to ensure WWC’s Systems security. It is the responsibility of every department to administer and act in accordance with the AUP. |

## Applicable Laws/Guidance

|  |  |
| --- | --- |
|  | This policy is in accordance with the Acceptable Use policy governed by ISO/IEC 27001 section A.7.1.3, describes the acceptable and nonacceptable uses of the organization’s resources. |

## Effective Date

|  |  |
| --- | --- |
|  | This policy takes effect the day after, Chief Information Officer (CIO), signs it and remains in effects until officially superseded or canceled by the CIO. |

## Approved

|  |  |
| --- | --- |
|  | The Chief Executive Officer |

## Associated Resources

|  |  |
| --- | --- |
|  | AUP 100 Email Use Policy in accordance with ISO/IEC 27002 section A.10.8.4  AUP 200 Internet/ Intranet Use Policy in accordance with ISO/IEC 27002 section A.12.1.1  AUP 300 BYOD Use Policy in accordance with ISO/IEC 27001 section A.11.7  AUP 400 Social Media Use Policy in accordance with ISO/IEC 27001 section 10.7 |

|  |  |
| --- | --- |
| Data Security Guidelines | |
| Section 1- Purpose  This document provides guidance and advice in helping Wilbur’s Widgets Company (WWC) to meet the control requirements for encrypted data on or in the cloud, company computers or personal device storage standards.   1. These guidelines set out WWC information security practice regarding confidentiality, integrity, and availability of all information data systems and should be read in accordance with ISO/IEC FDIS 27002 section 15 compliance, is used to avoid breaches of any law, statutory, regulatory, or contractual obligations and of any security requirement. 2. Provide clear direction to authorized users about requirements in protecting WWC’s information asset from inappropriate use, modification, loss, or disclosure. 3. Appropriate security standards and measures must be established, implemented, monitored, reviewed, and improved as required, to make sure that WWC’s information security management documentation framework and business objectives are met. | |
| Section 2-Background  This document was developed to support data security policy. Based on ISO/IEC FDIS 27002 section 15 compliance  Definition  *“Users” are anyone who has access to any of WWC’s IT system.*  *Public Data: data that is freely accessible to the data i.e., all employees/company personnel. This data can be freely used, reused, and redistributed without repercussion.*  *Internal-only Data: Data that is strictly accessible to internal company personnel or internal employees who has authorization to access it.*  *Confidential Data: Access to confidential data requires specific authorization and/or clearance. This covers social security numbers, cardholder data and more.*  *Restricted Data: Intellectual property, proprietary information or research data and data protected by state and federal regulations* | |
| Section 3-Scope  This guidance applies to the use of public data, internal-only data, confidential data, and restricted data. | |
| Section 4-Guidance Section  Public Data:4.1  4.1a. Data must be secured on company computer or personal devices with a user and password security feature.  4.1b. Data stored in the cloud must be backed up on the company server within DMZ to protect against an attack in case of downed internet access and to be used as a backup.  4.1c. Only approved data may be used for public usage. This information includes finances such as sale reports reported to the Securities and Exchange Commission,  Internal-Only Data:4.2  4.2a. Data stored on internal servers must be encrypted and put into a DMZ.  4.2b. Data stored on company computer or personal devices must be secured on the hard drive and encrypted.  4.2.3c. Data that is emailed outside the company or brought in will be scanned for viruses and malware.  Confidential Data:4.3  4.3a. Data with high priority must be sent with an encryption to protect confidentiality.  4.3b. Data stored in the cloud must be accessible from company servers in case files needs to be backed up or in the case of a full system recovery.  4.3c: Data stored on company computers or personal devices must be stored in a virtual vault to protect the company, customer, and intellectual property.  Restricted Data:4.4  4.4a. Restricted data regardless of storage on company computer, personal devices or cloud is not allowed to be copied onto any USB port, flash drives, external storage drive, CD, DVD, SD card, tertiary storage, or any other removable devices.  4.4b. Restricted data is prohibited from being printed and given to anyone that is not authorized by federal or state to have access.  4.4c. Data must be always encrypted unless while being viewed by an authorized user. | |
| Section 5-Roles and Responsibilities  All WWC’s Users are responsible for adhering to the policies and guidelines to ensure WWC’s Systems security. It is the responsibility of every department to administer and act in accordance with ISO/IEC FDIS 27002 section 15 compliance. | |
|  |  |
| Section 6- Effective Date  This policy takes effect the day after, Chief Information Officer (CIO), signs it and remains in effects until officially superseded or canceled by the CIO. | |
|  | |
| Section 7- Information and Assistance  Contact the Information Security Officer or HR for further information regarding this document. | |

**Section 8- Approved**

The Chief Executive Officer

Associated Resources

ISO/IEC FDIS 27002

**Implementation Plan**

|  |  |  |  |
| --- | --- | --- | --- |
| Policy to Implement | Definition | Justification | Responsibility |
| Asset Inventory Policy | This is based upon ISO/IEC FDIS 27002 section 7.1.1. Inventories of assets help to ensure that effective asset protection takes place, and may also be required for other business purposes, such as health and safety, insurance or financial (asset management) reasons. The process of compiling an inventory of assets is an important prerequisite of risk management. This policy will help WWC to establish an inventory of all assets and to put into place a maintenance schedule for applying patch management and updating out of date hardware and software. | WWC is running an outdated Operating System Windows XP. Microsoft is no longer providing supports, patching to fill the security gap, and is obsolete and non-compatible with newer processors and programs. | IT Department is responsible for handling the inventory and the configuration and patching of all devices, hardware, and software. |

Implementing this policy will help establish a controls and proper configurations to tighten security. To implement this policy all IT team members from the CISO all the way down to help desk must be trained and a culture of security must be created. The best way to implement this policy is to have a webinar or seminar where patching and configuration protocols and procedures are combed over and where standards and expectations are developed and onboarded into the day-to-day tasks within the IT department. WWC will benefit from implementing this policy because it will put them in a more stable and stronger security practice which in turn will show stakeholders, CEOs, and the board of directors that the company are being proactive and a good steward of WWC’s assets and bottom-line when it comes to legality.

**Asset Inventory Policy Life Cycle Plan**

The above diagram is based upon the Asset Inventory Policy recommended for Wilbur’s Widgets Company. WWC needs a road map to guide them in a clear concise direction towards regulation compliance. The asset inventory policy is based upon the ISO/IEC 27002 regulation section A.7.1.1. It helps a company create controls and protocol that take assets and put it into an inventory database. When WWC creates this list, they will then be in position to create a process in which all listed hardware, software and devices are properly configured, patched/ updated and or upgraded. The diagram walks through the steps needed and builds onto the next. Stated risks of not complying will result with openings within the network security. Assets inventory policy is being highlighted within this report because it is of high priority and needs to be addresses immediately. The threats are that WWC will be attacked due to an outdated operating system, Windows XP. Walking though the diagram the risk is stated along with the compliance that we are aiming to meet and the threat(s) if not addressed and resolved. For this life cycle to work executive buy is important. There will be a cost associated with the buying and licenses needed for the current operating system, but it is worth the expense in the end because with a new operating system, the current security protocols and configurations will be available to WWC. With the new operating system staying current with the latest virus and malware dictionary and protection will be easier to implement. Unlike other policies that requires all team members of a company to be aware asset inventory policy, only the IT department needs to be trained and aware of the implantation of the life cycle. By only training the IT department is lowers the risk of other departments knowing about potential security gaps and exploiting them. The end goal of this life cycle is to one lay the groundwork for the other recommended policies and two to create and maintain compliances with the industry standards and to be able to give WWC a stronger security stance.



References

Johnson, R., & Easttom, C. (2021). *Security policies and implementation issues* (3rd ed., pp. 80-81). Burlington MA: Jones & Bartlett Learning.

Policy.csu.edu.au. 2022. *Information Security Guidelines / Document / CSU Policy Library*. [online] Available at: <https://policy.csu.edu.au/document/view-current.php?id=470> [Accessed 4 April 2022].

Practices, B. and Template, D., 2022. *Data Security Policy Template*. [online] Netwrix. Available at: <https://www.netwrix.com/data\_security\_policy\_template.html> [Accessed 4 April 2022].

Nieles, M., Dempsey, K., & Pillitteri, V. (2017). An Introduction to Information Security. Retrieved 13 March 2022, from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf#page7>

Williams, B. (2013). *Information Security Policy Development for Compliance ISO/IES 27001, NIST SP 800-53, HIPPA Standard, PCI DSS V2 AND AUP V5*[Ebook]. Boca Raton, Florida: CRC Press Taylor & Francis Group.

Acceptable Use Policy. (2022). Retrieved 27 March 2022, from https://studylib.net/doc/18208070/acceptable-use-policy

(2012). Retrieved 27 March 2022, from <https://www.michigan.gov/-/media/Project/Websites/msp/cjic/pdfs7/Acceptable_Use_Policy.pdf?rev=92ed3b3dd19749358f6f6613f04ac254>

Johnson, R., & Easttom, C. (2021). *Security policies and implementation issues* (3rd ed., pp. 80-81). Burlington MA: Jones & Bartlett Learning.

Shah, N. (2020). 3 Important Measures for WAN Security with SD-WAN | Fortinet Blog. Retrieved 11 April 2022, from https://www.fortinet.com/blog/industry-trends/prioritizing-concerns-around-wan-security-issues

Wilkins, S. (2011). Common Wireless Network Security Threats. Retrieved 11 April 2022, from https://www.pluralsight.com/blog/it-ops/wireless-lan-security-threats