7COM1066-0901-2023

INFORMATION SECURITY, MANAGEMENT, AND COMPLIANCE.

NOVEMBER 2023.

ABSRTARCT

These abstract summaries the basic methods for managing an organization's safe digital infrastructure. It emphasizes the significance of using firewalls, antivirus software, and intrusion detection systems to prevent unauthorized access and cyber assaults. It also emphasizes the importance of staff training on digital security best practices, safe password rules, and multi-factor authentication to improve overall security. It also emphasizes the significance of doing security checks and inspections on a frequent basis to detect and mitigate vulnerabilities in the digital infrastructure. These steps, taken together, add to the organization's strong and initiative-taking approach to cybersecurity.

INTRODUCTION

After gathering information on the incident which took place in the police service Northern Ireland (PSNI), the information of 10,000 police officers was published on a public website 'whatdotheyknow' on the 8th of August 2023, following the requirement of the FOI.

On this day, the PSNI was pained due to the information breach, the information was breached because of FOI. Data containing serving officers' and staff's names, the initials, ranks/grades, duties, service numbers, departments, locations, duty types, and genders, was published on a legit website known as www.whatdotheyknow.com. Due to the continuous threat, the incident was made public on August 9th, 2023. This incident of information breach has made members of the PSNI, both the staff and serving officers lose Confidentiality and integrity. Information cannot be managed by the members of PSNI. Their partners and communities have lost trust in the police department of Northern Ireland. (www.psni.police.uk, 2023)

1.1 BACKGROUND

The PSNI was founded in 2001, replacing the Royal Ulster Constabulary (RUC). The RUC has been serving the people of Northern Ireland as their policing organization since 1922. The aim of creating PSNI is to keep the safety of the community. They deal with organized crime, terrorism, and sectarian tension. (RUTTER, 2023)

1.1.1 FREEDOM OF INFORMATION (FOI) ACT

The FOI was started in the United States in the year 1996, letting the public have access to federal agency information. This is to show the transparency of information within the country. Citizens will be able to check the work of their government. (Ben, 2017).

1.1.2 WHY IS POLICY NEEDED?

The policy is a set of rules governing any organization, the PSNI need a new policy about information handling. The policy will be based on past incident rule changes, legal and regulatory requirements, and security concerns.

Changing policy will advance the PSNI member's knowledge of technology, the way information is stored, shared, and accessed, and to make sure information is secure. New rules need to be in place that all members of the PSNI must follow. In addition, developing a new policy for PSNI will ensure that information will be securely stored, shared, and accessed. (Jakob & Fagerberg, 2017)

1.2 PURPOSE

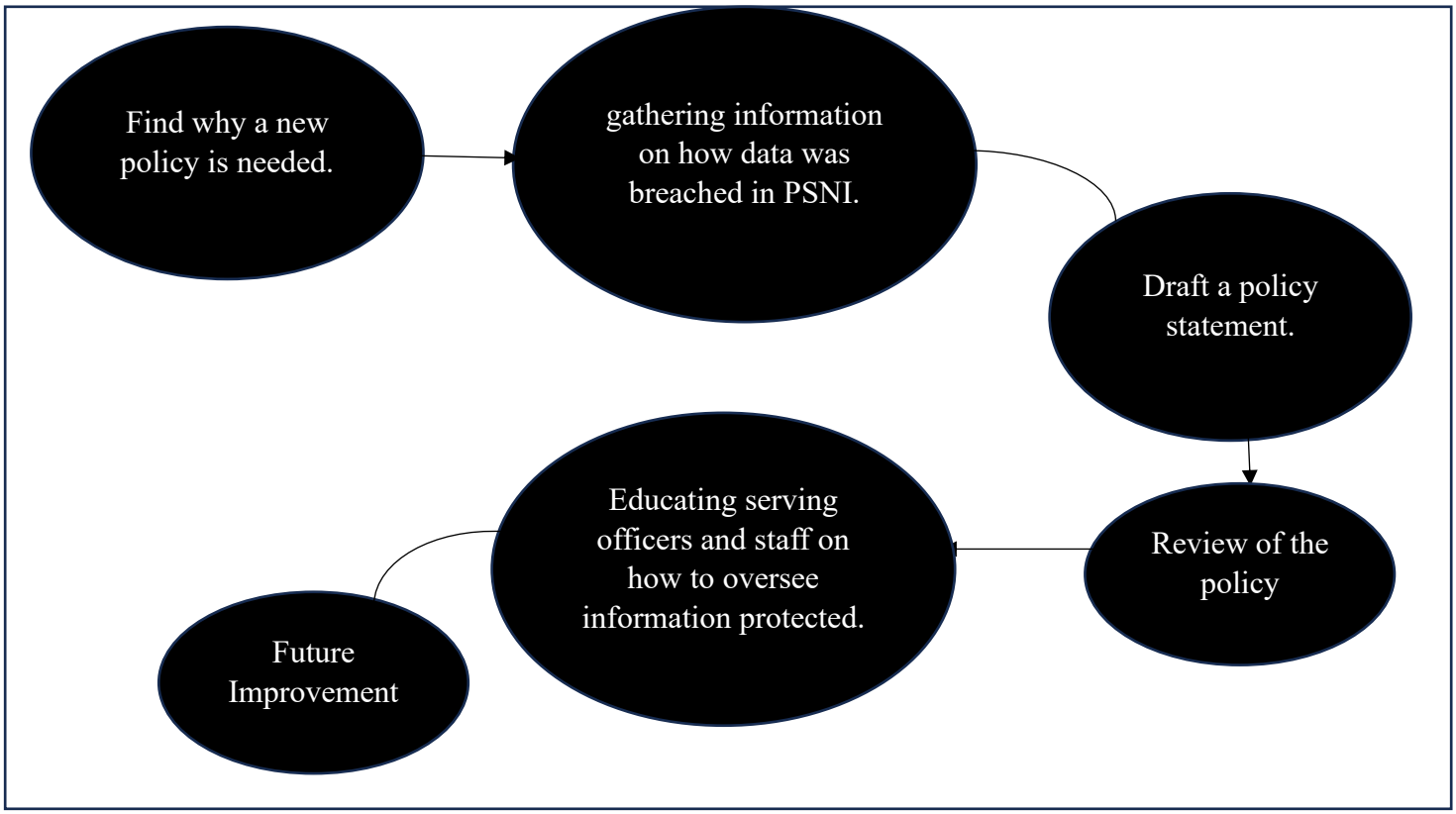
The focus of this policy is to develop clear policy guidance on how information should be managed. This aims to protect information, ensure only authorized people have access to information and keep the confidentiality, integrity, and availability of the PSNI.

1.3 SCOPE

This policy is to ensure information is protected, this policy will include giving access to information related to the operation and decision-making process of PSNI by the authorized user only.

1.4 METHODOLOGY

The structure below shows the steps in developing a standard policy for PSNI.



CONTEXT ESTABLISHMENT

Establishing context for the PSNI policy, its aims to protect information, manage risk, analysis risk and developing of policy for the organization, we would be looking at various angle in making sure the PSNI organization are overseeing information appropriately. the external, internal environment, risk management approach, risk evaluation criteria and impact criteria, scope and boundaries, organization for information security risk management will be the factors used to analyses the risk.

2.1. EXTERNAL ENVIRONMENT

It is essential to review the environment in which the PSNI functions, several variables are given that must be considered while creating the risk assessment.

- **Transparency:** The PSNI needs to make the operation transparent, and in deciding process, it must respect the necessary for protecting information.
- **Accountability:** The PSNI will oversee the public and the answering to the FOI request in a responsible manner.
- **Duty to protect:** The PSNI must ensure the protection of its information.
- **Compliance with legislation:** The PSNI must follow the rules and regulation of the FOI request.
- **Respect for individuals' rights:** The PSNI must ensure the protect the privacy of its member.
- **Continuous improvement:** The PSNI must continuously improving on their process for addressing the FOI request.

2.2. INTERNAL ENVIROMENT

- **Training and support:** the PASNI will give right resources to effectively manage and react to freedom of information inquiries on time.
- **Resources:** The PSNI is going to analyze its methods for getting freedom of information inquiries on a regular basis to discover areas for development and assure that they follow regulations.
- **Review processes:** The PSNI will share information freely with the public about its freedom of information operations and will give clear instructions on how to send inquiries.
- **Communication:** the PSNI will work together alongside other government departments and stakeholder to impart best practices to strengthen its policy of accountability and transparency.
- **Public engagement:** the PSNI will engage with the public to learn about their information demands and concerns and take them into consideration while dealing with freedom of information demands.

2.3. RISK MANAGEMENT APPROACH

This explains the risk management activity’s aims and goals, as week as how it will be done, who is going to be accountable for each part, and what is addressed.

- **Risk assessment:** the PSNI will conduct frequent risk assessment to discover potential threats and issues when dealing with freedom of information inquires and implement measures to mitigate this risk.
- **Compliance monitoring:** to make sure that all inquiries are addressed by regulations and standard practices, the PSNI will keep track of the implementation of freedom of information law and its internal processes.
- **Training and support:** the PSNI will offer continuing training and help to staff members who process freedom of information inquires, ensuring that they have the skills to deal with any danger or issues.
- **Continuous improvement:** the PSNI will continually evaluate and improve its risk management approach to dealing with freedom of information inquires, taking account of stakeholder feedback and prior experiences.

2.4. RISK EVALUATION CRITERIA AND IMPACT CRITERIA

2.4.1. RISK EVALUATION CRITERIA

- **Likelihood of occurrence:** what likelihood is the risk in the handling of freedom of information act inquires?
- **Impact on operations:** which impact will the risk have on the PSNI's ability to process freedom of information inquires properly?
- **Impact on public trust:** what impact will the risk have on the public's confidence in PSNI's transparency and responsibility?
- **Legal and regulatory implications:** what are the regulatory and legal consequences of the risk?
- **Reputational impact:** how will the risk affect the PSNI's trust when dealing with FOI inquires?

2.4.2. IMPACT CRITERIA

- **High impact:** risk which could compromise the PSNI's ability to manage freedom of information inquires and have a severe impact on public confidence and credibility.
- **Medium impact:** risk which could disturb the PSNI's processing freedom of information inquires and have insignificant effect on public confidence and credibility.
- **Minimal impact:** risk that could have a small impact on public confidence and credibility while causing slight delay to the PSNI's handling of freedom of information inquires.

Using these guidelines, the PSNI will successfully analyses and priorities risk in dealing with freedom of information requests, in addition to create suitable mitigation method.

2.5. RISK ACCEPTANCE CRITERIA

- **Legal and regulatory compliance:** risk which do not fulfill legal and regulatory requirement are going to be denied.
- **Operational impact:** risk which threaten the PSNI's ability to process freedom of information request will be denied.
- **Likelihood and severity:** risk which are not capable of being successfully minimized or controlled will not be approved.

- **Mitigation measures:** Risks that cannot be effectively mitigated or managed will not be accepted.

  The PNSI may ensure that only acceptable risk is taken in the handling of freedom of information request by applying these acceptance criteria.

2.6. SCOPE AND LIMITS

The PSNI's scope and limits in responding to freedom of information requests include:

- **Compliance with legal and regulatory requirements:** the PSNI must guarantee that any steps taken in reaction to FOI requests are done by the relevant legislation and rules.
- **Operational impact:** the PSNI must consider the possible practical consequence of dealing with freedom of information request, including any obstacles to it is the ability to perform its duties.
- **Likelihood and severity:** to decide their acceptance, the PSNI needs to decide the decide the likelihood and severity of risk related to processing freedom of information requests.
- **Mitigation measures:** to oversee and reduce the risk involved with responding to freedom of information request, the PSNI must have suitable mitigation methods in place.

By explicitly outlining the scope and bonds for addressing freedom of information requests, the PSNI can ensure that it actions are consistent with its legal and ethical obligations, as well as that it keeps public trust and confidence on its operations.

2.7. ORGANIZATION FOR INFORMATION SECURITY RISK MANAGEMENT

- **Information security:** The PSNI must ensure that all information released in response to Freedom of Information requests is oversaw securely to protect sensitive and confidential information.
- **Transparency and accountability:** The PSNI must prioritize transparency and accountability in its handling of Freedom of Information requests, ensuring that it supplies correct and prompt information to the public.
- **Privacy considerations:** The PSNI must consider the privacy implications of releasing certain information in response to Freedom of Information requests and respond appropriately to protect individuals' privacy rights.
- **Continuous improvement:** The PSNI should regularly review and evaluate its processes for handling Freedom of Information requests, seeking opportunities for improvement and implementing best practices to enhance efficiency and effectiveness

RISK ASSESSMENT

3.1. Risk ASSESSMENT TABLE

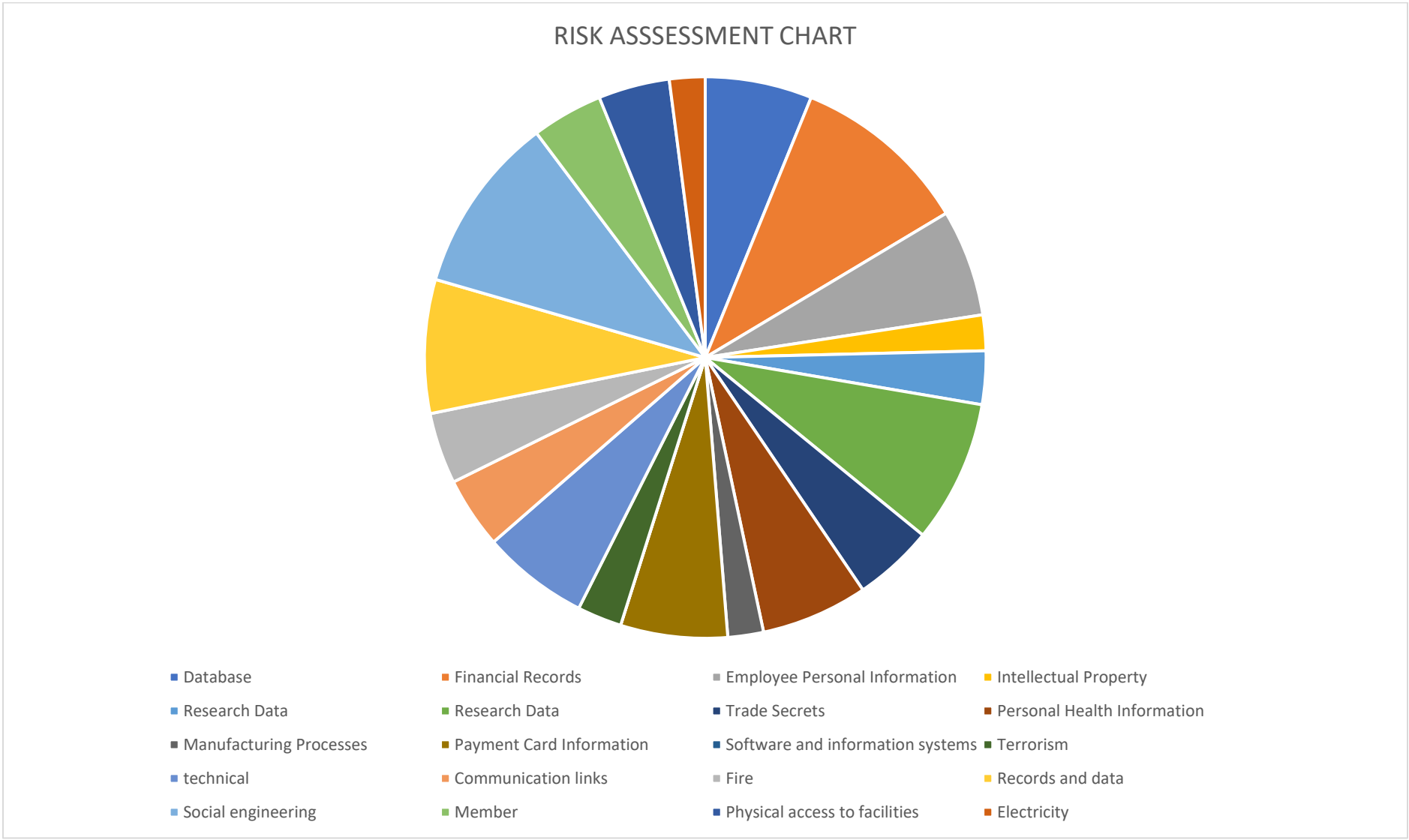
Asset	Vulnerability	Vulnerability code	CIA	Threat code	Con. rating	Likelihood rating	R = C x L	Risk treatment	Mitigation	Control domain from ISO 27002 and its type	Revised likelihood rating	Residual Risk rating	Risk acceptance states	your relevant policy statement number addressing the control
PSNI Database	Information Disclosure	CVE-2021-21468	Unauthorized access to the database information could be cut or false information could be added.	TT02, TH10	4	3	12	Avoid	Implement access controls and encryption to restrict unauthorized access	preventive	1	2	Very low	4.5.1
PSNI Financial Records	Data Leakage	CVE-2020-35992	PSNI members could face physical threats.	TT03	5	4	20	Avoid	Utilize data loss prevention tools to check and prevent unauthorized transmission of financial records.	preventive	1	2	Very low	4.5.9
PSNI Employee Personal Information	Privacy Violation	CVE-2022-29613	Ransome could be asked from the organization.	TT03	3	4	12	Avoid	Encrypt employee personal information to protect it from unauthorized access.	Preventive	2	2	medium	4.5.5
Intellectual Property	Data Exposure	CVE-2023-4828	Destruction and corruption of the database could happen.	TH02	2	2	4	Reduce	Monitor and restrict the transfer of intellectual property outside of authorized networks.	detective	1	1	Very Low	4.5.5
Research Data	Information Leakage	CVE-2020-5799	It could increase the chance of theft, ransomware, and data breaches.	TT03	2	3	6	Reduce	Implement data loss prevention tools to check and prevent the unauthorized transmission of research data.	preventive	1	3	low	4.5.5
PSNI Confidential Documents	Sensitive Data Disclosure	CVE-2023-33989	It could damage your reputation.	TT02, TH10	4	4	16		Implement strong access controls and encryption to protect confidential documents from unauthorized disclosure.	preventive	1	2	Very low	4.5.2
Trade Secrets	Confidential Information Disclosure	CVE-2023-6105	It could damage PSNI service.	TT02, TH10	3	3	9	Reduce	Implement strict access controls and encryption to protect trade secrets from unauthorized disclosure.	preventive	1	3	low	4.5.2

PSNI Personal Health Information	Unauthorized Data Access	CVE-2022-47376	It could compromise personal information and trend secrets.	TH02, TH16	4	3	12	Avoid	Encrypt personal health information to protect it from unauthorized access.	preventive	1	4	medium	4.5.1
Manufacturing Processes	Data Manipulation	CVE-2021-3971	It could cause the communities not to trust the organization.	TT03	2	2	4	Reduce	Implement strict access controls and encryption to protect manufacturing processes from unauthorized manipulation.	preventive	1	3	low	4.5.9
PSNI Payment Card Information	Data Breach	CVE-2023-41962		TT03	4	3	12	Avoid	Utilize tokenization and encryption to protect payment card information from unauthorized access.	corrective	1	2	Very low	4.5.7
Software and information systems	Unauthorized use of software	CVE-2023-46725	Software that is not authorized could affect the organization, as information stored on it might be leaked.	TH19	4	2	8	Reduce	Implement access control policies, use software with proper licenses, and regularly check usage logs to detect any unauthorized use of software.	corrective	1	1	low	4.5.10
Terrorism	Bomb attack	CVE-2023-3782	It could cause death for serving officers, staff, and other members of PSNI, and loss of sensitive information.		5	1	5	Reduce	Implement physical security measures like security cameras, access control systems, and regular security drills.	preventive	1	3	low	4.5.1
technical	Errors in maintenance, Software errors	CVE-2023-5723, CVE-2023-20082	Software errors could result in loss of data and software crashes.	TT01	4	3	12	Avoid	Train maintenance staff properly, implement regular maintenance schedules, and perform regular audits. Regularly update software, test software updates before implementation, and have a disaster recovery plan.	corrective	1	3	low	
Communication links	Failure of communication links	CVE-2022-29237	This could affect in terms of not completing a task or misunderstanding	TI03	4	2	8	Reduce	Implement redundant communication links, regularly evaluate communication links, and have backup	corrective	3	2	Medium	

			a specific instruction.						communication plans.					
Fire	physical damage to infrastructure and systems	CVE-2021-2138	It could reduce access to a certain resource.	TP01	4	2	8	Reduce	store backups in off-site locations.	corrective	1	1	Very low	4.5.1
Records and data	Falsification of records	CVE-2023-47801	It could mislead in research on records.	TC03	5	3	15	Avoid	Implement access control policies, regularly audit records, and have a reporting system for any suspicious activity.	protective	1	3	low	
Electricity	Loss of electricity	CVE-2023-5506	It could affect the flow of information and operations going on	TI01	4	1	4	Reduce	Implement backup power systems, regularly assess backup power systems, and have a plan for restoring power.	protective	1	2	Very low	
Social engineering	Disclosure of information	CVE-2023-6105	It could result in the termination of employees, loss of trust, and loss of the relationship.	TH10, TH02	5	4	20	Avoid	Educate employees on social engineering tactics, implement access control policies, and have a reporting system for any suspicious activity.	corrective	1	2	Very low	4.5.1
Member	• Misuse of information systems • Unintentional change of data in an information system	CVE-2023-40586, CVE-2023-44315	it could result in including information, which is not meant to be added.	TH13, TC01	4	2	8	Reduce	Implement access control policies, regularly check usage logs, and have a reporting system for any suspicious activity.	protective	2	3	Medium	4.5.7
Physical access to facilities	Unauthorized physical access	CVE-2023-5409	it could lead to loss of data and financial record loss.	TH17	2	4	8	Avoid	Implement physical security measures like security cameras, access control systems, and regular security drills.	protective	1	1	Very low	4.5.1

Looking at the above vulnerabilities, digital assets will be able to be safeguarded and be prevented from unauthorized access, information disclosure, sniffing, data breaches, malware attacks etc. All serving officers, staff, and partners should be trained to keep the integrity of information and to make the digital environment more secure. This vulnerability will make sure the PSNI digital environment is secure, and information is protected.

3.2. RISK ASSESSMENT CHART



The chart above shows how the outcome of both the consequence of a vulnerability and the likelihood of the vulnerability happening. PSNI should focus more on the Financial, Database, terrorism attacks, and software and information systems. Due to my research, the organization will face threats in this section. PSNI serving officers and staff should be trained on how to keep information protected.

PSNI POLICY STATEMENT

SECURE ACCESS AND DOCUMENT MANAGEMENT POLICY

4.1. Policy Statement

The Police Service Northern Ireland (PSNI) commits to supplying efficient and effective policing aid to the community. Our policies aim to ensure our ability to act with integrity, transparency, and an ethic of respect. We are committed to advancing the rule of regulation and protecting the freedoms and rights of any individual. Our law enforcement personnel receive training to exercise their authority effectively and to treat all members of the public equally and with respect.

4.2. PURPOSE

The focus of this policy is to develop clear policy guidance on how information should be managed. This aims to protect information, ensure only authorized people have access to information and keep the confidentiality, integrity, and availability of the PSNI:

- **Information should be available when needed:** when information is needed it should be available to be used.
- **An authorized person should access information:** An authorized person should easily find information.
- **Information should be able to be interpreted:** information should be able to find any recent changes when it was made, where it was changed, by whom it was changed, and the day and time it was changed.
- **Information should be trusted:** information should keep its integrity, and when it is in use it should still produce the original content.
- **Information should be kept** information should be checked and updated so, as not to experience the earlier data breach incident.
- **Information should be secure:** information should be kept in a protected environment. And it should be heavily encrypted in case of any data breaches.
- **Information should be set to reading format only:** after making any changes to the information, it should be set to read-only, this will minimize the risk of error handling by the user.
- **Information should be recovered and destroyed appropriately:** in case of a user mistaking information, it should be easy to get information back in doing this information needs to be backed up in a secure environment, and while destroying information make sure it follows the procedure. Failure to do this, in the cause of destroying information, might fall into the possession of an unauthorized person.

4.3. SCOPE

This policy is to ensure information is protected, this policy will include giving access to information related to the operation and decision-making process of PSNI by the authorized user only. The new policy will ensure all serving and staff are well trained and educated on the use of the new policy, following the requirement of the FOI and how it should be responded to. In addition, the scope will ensure that the open government and access to information are contained within the PSNI organization.

4.4. STANDARDS

ISO standards related to the Police Service of Northern Ireland (PSNI) may include:

- **ISO 9001:2015 - Quality management systems**
  The ISO 9001 crate standards for quality management systems for organization. (iso, 2015)
- **ISO/IEC 27001:2022 - Information security management systems** This document describes the criteria for creating, implementing, keeping, and upgrading an information security management system within the context of the organization. This paper also offers specific standards for assessing and treating information security issues. (iso, 2015)
- **ISO 45002:2023 - Occupational health and safety management systems**
  This standard supplies a set of rules on developing, implementing, maintenance, and continuous improvement of occupational health and safety management system. (iso, 2015)
- **ISO 22301:2019 - Business continuity management systems**
  This standard creates the requirement for implementing, keeping, and improving a management system to prevent reduce the likelihood of planning, Responding, recovering from disruptions. (iso, 2015)
- **ISO 31000:2018 - Risk management principles and guidelines**

  supplies guidelines for businesses to use in risk management. These concepts can be adapted to each organization's unique needs. ISO 31000:2018 sets up comprehensive understanding, strategic decision-making, operational excellence, an initiative-taking approach, and stakeholder confidence as standards. (iso, 2015)

  These standards can help the PSNI ensure the effectiveness, efficiency, and safety of their operations, as well as prove their commitment to continuous improvement and best practices in various aspects of their work.

4.5. Guidelines

4.5.1. Access Control

- The PSNI document, system, and network should be accessed by authorized users only.
- Access to the system, network and documents should be allowed to specific people where they can perform their necessary duties.
- Reviewing of access should be reviewed regularly.
- Sharing of accounts should be forbidden and unique, accounts should be created for individuals.
- Using of strong password should be made mandatory for all the users.
- Accessing sensitive information, the use of authentication should be used.
- Any failed login attempt should be checked.
- Install physical security measures, such as surveillance cameras, access control system, and regular security and fire drills.
- regularly check usage logs and have a reporting system for any suspicious activity.

4.5.2. Document Classification and Handling

- The classification of sensitivity level e.g., the public restricted and confidential document, should follow the classification framework of PSNI.
- Classifying of document by labeling it appropriately, should be made by the owner.

- Access control should be implemented to restrict any unauthorized user.
- Creation of control mechanisms should be made. To make sure the information is correct, and it keep its integrity.
- Document should be stored in the proper repository and must be encrypted.
- The retrieving and deletion of document policy should be well defined and followed, to make sure legal and regulatory requirements are met.

4.5.3. Document Sharing and Transmission

- Sensitive information should be encrypted, or the use of a secure file protocol should be in place before sharing any document.
- Authorization from other bodies should be made before sharing any document.
- The use of A watermark should be used on every single document, so information will not be manipulated.
- Any document sharing with partners should be made clear of no disclosure.

4.5.4. Document Backup and Recovery

- PSNI documents must be backed up regularly to keep their integrity and accuracy.
- Backup document should not be kept in the same repository as the original document, it should be kept off-site for physical damage or cyber threat.
- Document recovery procedure should be used, and it must be assessed to make sure the restoration of the document is correct.

4.5.5. Digital prevention

- It is the responsibility of all PSNI serving officers, staff, and partners to prevent unauthorized access, digital security risk, data breaches and social engineering. They must follow the secure procedure for overseeing information, transferring, and sharing digital information while using encrypted, staff, partners and officers need to be trained and educated and members to keep up to date with the latest digital prevention technology.

4.5.6. Folder structure naming

- All the digital information should be named clearly for organizing and retrieval of information, any name not following the PSNI naming structure should be automatically removed.

4.5.7. Risk Management:

- Find, assess, and manage risks effectively.
- Implement comprehensive risk management policies and procedures.
- Continuously check risks and take necessary actions to mitigate them.

4.5.8. Information storage

- All information should be stored in a reliable storage system. E.g., are encrypted servers or the computer cloud platforms (OpenStack, cloud stack.). also, regularly back up information.

4.5.9. Handing and transferring of Information

- PSNI members should always follow the secure protocol to ensure sensitive data are not accessible by unauthorized users. The use of encrypted channels, secure file transfer, and password-protected files should be included.

4.5.10. Education and Training

- Digital prevention, data security, privacy protection, and cyber threat awareness should be taught to all the members of PSNI. Regular training should be conducted at least every six months, to know the latest vulnerability and how to prevent it.

4.6. Compliance

- PSNI employees, contractors, and other authorized individuals shall follow this policy.
- Non-compliance with this policy may result in disciplinary actions, including termination of employment or legal consequences.

4.7.Policy Review

- This policy shall be reviewed annually or whenever significant changes occur in the organization's environment, legal requirements, or industry standards.

These guidelines should serve as a foundation for Police Service Northern Ireland (PSNI) policy framework. It is essential to communicate these policies clearly to all employees and regularly train them to ensure compliance and keep a strong organizational culture.

5.0 CONCLUSION

In conclusion, organizations must priorities cybersecurity measures to guard against cyber-attacks and vulnerabilities. Businesses can dramatically minimize the likelihood of unauthorized access and cyber-attacks by regularly updating and patching software, implementing firewalls and antivirus software, training employees on digital security best practices, enforcing secure password policies, and conducting regular security audits. In today's increasingly linked world, these initiative-taking steps are critical for securing sensitive information and ensuring the integrity of digital infrastructure.

References

Ben, W., 2017. *The Politics of Freedom of Information : How and Why Governments Pass Laws That Threaten Their Power.* 1 ed. s.l.:Manchester University Press.

iso, 2015. *iso.* [Online]
Available at: www.iso.org
[Accessed 15 Novemvber 2023].

Jakob, E. & Fagerberg, J., 2017. *Innovation Policy: What, Why, and How." Oxford Review of Economic Policy.* [Online]
Available at: JSTOR, http://www.jstor.org/stable/26363353
[Accessed 16th November 2023].

P, A. G. & Smith., W. C., 1994. Developing police policy: An evaluation of the control principle. *Am. J. Police,* Volume 13, p. 1.

Pozen, D. E., 2017. Freedom of information beyond the Freedom of Information Act. 165(5).

RUTTER, J., 2023. *instituteforgovernment.* [Online]
Available at: www.instituteforgovernment.org.uk
[Accessed 10 Noverber 2023].

www.psni.police.uk, 2023. *psni.police.* [Online]
Available at: www.psni.police.uk
[Accessed 13 November 2023].