Group 3 Final copy.docx

by Aqib AMIN

Submission date: 25-Aug-2021 09:04PM (UTC+0100)
Submission ID: 159186166
File name: Group_3_Final_copy.docx (42.1K)
Word count: 3196
Character count: 18697

Information Governance and Cyber Security

Group Task

By

Aleksander Peshev,
Aqib Amin,
David Alechenu Odaudu
Ivan Zaytsev,
Maria Angelica Nunez

GROUP 3

Module Number	LD7087
Tutor Name	Ms. Rose Fong
Programme	MSc. Computing & Technology

S/N	Name	Student No.	Part
1	Aqib Amin	w20051393	Introduction, Aims, Scope and Policies
2	Aleksander Peshev	w20050668	Roles & Responsibilities
3	Maria Angelica Nunez	w19028386	Information Governance Implementation Plan
4	Ivan Zaytsev	w20051320	Information Governance-Monitoring Mechanisms
5	David Alechenu Odaudu	w20056485	How to Mitigate Security Vulnerabilities and Conclusion
GROUP 3			

could also mention the word count

Contents

1. Introduction 4
2. Purpose 4
3. Scope 4
4. Roles and Responsibilities 5
5. IG Policies for University of Higher Education (UHE) 7
6. Implementation Plan 8
7. Information Governance - monitoring mechanisms. 11
   7.1 Audit 11
   7.2 Training 11
   7.3 Data protection monitoring 12
8. How to Mitigate Security Vulnerabilities 12
9. Conclusion 14
10. Approval Table 14
References 15

1. Introduction

Information security is very vital for each organization as they operate confidential data. Every business sector is now focusing more on how to keep their data safe from every bad aspect. Nowadays, educational institutes are focusing more on the information security framework after the cyber-attack on the blackboard back in 2020. The University of Higher Education (UHE) wants us to develop an information security policies framework for their Information security management system (ISMS). This is the group activity in which every member has a specific role in the development of this framework. In this report, we will describe the purpose and scope of these policies and will mention different roles and their responsibilities in order to implement these policies in a clear way. In addition to that, different monitoring mechanisms will also be discussed to check and balance the information security policies to avoid any security vulnerabilities.

2. Purpose

The purpose of this Information Security Policy is to enable UHE to meet the requirements of ISMS so that all the students and staff will have the confidence that their information is handled with great care. This report will educate all the staff of the university about the policies and will clarify their responsibilities towards information governance. The intention of this report is that the UHE meets all the legal and ethical obligations involved in managing the records. This means that they will be known how to use the personal information of the students or staff, when to share the information with any third party and under which circumstances (Ismail et al., 2017).

3. Scope

This document applies to all employees, students of the UHE, and other third parties who are using or have access to UHE information. This framework covers all the data held by

UHE in the form of soft or hard form, records communicated through networks, letters send through fax or any other similar method, visual and photographic materials including slides and CCTV recording, and all types of conversation such as spoken, voicemail, etc. (Imperial College London, 2021).

could also discuss the related operations

4. Roles and Responsibilities

The main purpose of information governance (IG) at education is to make sure that it has put the latest up to date IG policy and ensure it has been carried out. The IG board must make sure staff are trained in a way, so that they comply with the regulations about their roles and keep sensitive information private and confidential (University of Bristol, 2021). The IG board at university consists of the following roles:

- **The University's Information Management Group (IMG)** - **The Director of Information Security (DIS) will be responsible and accountable for the information governance policies and managing the cyber and information security** within the University of Higher Education (UHE). The IMG is also responsible for recommending policies, monitoring and reporting on compliance, as well as reporting any risks that have been passed by the UEB to them. The group is also responsible for overseeing every aspect of the IG policy, coordinating IG at University and raising awareness (University of Sheffield, 2021).

- **University Executive Board (UEB)** - is responsible for considering the strategies and policies that have been recommended by the Information Management Group (IMG) and whether they are agreed and designated by the board to the IMG (University of Sheffield, 2021).

- **University Secretary** - reports to UEB, for the extent of which the university is compliant with, if more actions are required, existing risks and if any further actions are required. The secretary has the responsibility to ensure that policies and

procedures are proposed and implemented, mechanisms are established for monitoring the policies effectiveness and report any potential risks and compliance (University of Sheffield, 2021).

- **Information Management Operation Group (IMOG)** - is the one that is responsible for developing and implementing policies and tasks given to them by IMG (University of Sheffield, 2021).

- **Data Governance Group** - its main responsibility is to oversee the University's Data Governance Structure, and make sure that is fit for purpose and harmonized across all platforms. Develop a consistent set of data procedures for data quality, form a task force for the developing of certain aspects of data governance. Lastly, to put a plan in place for the promotion and understating the benefits of good data governance policies (University of Sheffield, 2021).

- **Data Protection Officer (DPO)** - is an advisory role that helps Faculty and departments to comply with the data protection provisions. The DPO would provide information and advice on how to process all personal data. As well as training staff on how to do that and providing them with materials (University of Sheffield, 2021).

- **President or Vice-Chancellor** - who oversees the IG board, and the responsibility for the policies, decisions and their implementation by the board rests with the board through him.

could arrange the order of the role in term of their seniority

- **Senior Information Risk Owner (SIRO)** - is responsible for managing all information that is being processed by the university. This means that the SIRO ensures that the information is accurate, secured and legislation is complied with (University of Sheffield, 2021).

who is accountable for this?

- **Faculties and Departments** - their Vice Presidents and heads of departments are mainly responsible for the implementation of the university's IG policies and procedures within the departments assigned to them. **It is important to note that this into an extent includes the university's staf**f (University of Sheffield, 2021).

- **Information Users - those are all members of the university (Staff and Students)**. Each of them has a purpose and a role within the IG framework and responsibilities in regards to the information they hold (University of Sheffield, 2021).

5. IG Policies for University of Higher Education (UHE)

We propose Information Governance Policy framework for the UHE that surrounds the following IG Policies:

- **IGP-01 – Data Protection Policy**
  This policy defines how personal data is stored and used in the UHE. This involves setting up rules, principles, and guidelines to ensure that the data which the university holds is safe (Hina and Dominic, 2016).

- **IGP-02 – Records Management and Retention Policy**
  This policy involves the lifecycle of the records, which means how long the organization needs to store any document and when it should delete it from its system (Bhaharin et al., 2019).

- **IGP-03 – Digital Preservation Policy**
  This policy is about storing and managing digital records through a digital preservation strategy (Bhaharin et al., 2019).

- **IGP-04 – Personal Data Breach Policy**
  This policy defines the standards according to the GDPR to protect the rights of individual's data that how personal data is kept and processed. The organization takes the necessary measures to avoid unauthorized access (Zerlang, 2017).

- **IGP-05 – Information Security Policy**
  The aim of this policy is to protect student's records which are in different forms for example quiz, assignments marks. Staff personal data is also managed in a way that completely follows this policy (Zerlang, 2017).

- **IGP-06 – Information Sharing Policy**
  This policy involves the sharing of information with other people or a third-party organization. It consists of all legal and ethical considerations and the consent of the people is very important while in this policy (Zerlang, 2017).

- **IGP-07 – Privacy Impact Assessment Policy**
  This policy assesses all the impacts on the privacy of the individual and provides a solution to avoid any risks (Bhaharin et al., 2019).

good

6. Implementation Plan

IG is essential for setting standards and contributing to broad rules that maximise information access. The IMG leads the data governance process, and all participants must understand their roles and responsibilities. Therefore, to achieve effective information governance, the UHE secures the institutions data, maintain group content, choose a storage location, and versions. For which is necessary the following activities.

- **Establishment of a committee**

  The IMG will head this committee to examine the information's concerns and risks. According to Iannarelli & O'Shaughnessy (2015), The Committee should have a thorough understanding of the industry and the standards for successful operation.

- **Analyze potential policies**

  The IOMG, in collaboration with the UEB, will conduct an ongoing analysis of effective and ineffective policies. A comprehensive document that contains policies for resolving recorded issues (Kahn, 2009). Additionally, in collaboration with the Data Governance Group, the incidents that have harmed the university's reputation are analyzed.

  could recommend some policies here

- **Integral approach**

  The data governance structure was created with all University levels in mind to balance priorities, speed up conflict resolution, and promote data quality, and privacy protection. Although the commitment comes from top management. A strong managerial involvement is necessary for accomplishing long-term collective success (Smallwood, 2019). Whereas, the UHE will educate all Information Users on their roles and responsibilities within the organization.

- **Establish awareness and training throughout the University**

  Consistent governance compliance requires awareness, education, and training for all Users. Mandatory classes of IG can be required for the employees (Iannarelli & O'Shaughnessy, 2015). Security is a concern for everyone, not just IT. All institution employees' devices and app usage must be tracked. Personnel attitudes towards handling confidential University data will also be appraised.

- **Monitoring and evaluation**

  Effective IG demands continuous evaluation. Since IOMG will be evaluating continuously, the following questions will be asked periodically: What information should be safeguarded? Which risks are involved? As stated by Lomas (2010) It is crucial to monitor all risks continuously to provide information that is consistent with institutional and collective values. As a result, data will be classified, and policies, teams, and accountable individuals can be redefined.

- **Establishment of communication channels**

  Constant communication between the IT staff, Data Protection Officer, UEB, and an external advisor will be encouraged, as will discussion of recent global or industry-level incidents and the extent to which the UHE is prepared to prevent and respond in the event that this occurs. In order to address information issues or risks, it is a priority the support throughout a strong communication with the Board and Managers (Ragan, 2013). This results in performance measurement of information governance efforts, ensuring that objectives are met and resources are appropriately managed.
  Furthermore, all parties are encouraged to communicate openly. Transparent communication fosters trust, which contributes to the institution's increased visibility.

- **Promote agility and adaptability**

  New platforms impact the industry daily. Policies and guidelines can be changed. The UHE will answer the questions below. How does it work? What doesn't work? What can be done to improve? It is critical to implement adaptation strategies in order to incorporate larger perspectives into IG (Bednar, et al., 2018).

The UHE will employ this operational implementation strategy to ensure that the activities outlined below are carried out in an agile manner and that feedback is obtained during each interaction.

7. Information Governance - monitoring mechanisms.

7.1 Audit

The UHE University will implement a yearly audit to make sure its policy is up-to-date and comply with current legislation. All information governance and security policies and procedures will be audited and reviewed on a regular basis to verify that they are up-to-date, still fit for purpose, and that the UHE University is still in compliance. An audit should be a continuous effort by the organisation and the IG programme manager to monitor and ensure compliance (du Fresne, 2020). A yearly audit of IG procedures is intended to identify weaknesses and inefficiencies so that an organisation can avoid them in the future (Ma'ayan & Carmeli, 2015). Audits are used to ensure that information governance standards are being followed and, if required, to suggest high-level policy changes. In addition to the guidelines provided in ISO 19011, ISO/IEC 27007:2020 offers guidance on implementing an information security management system (ISMS) audit programme, performing audits, and the competence of ISMS auditors (www.iso.org, 2020).

7.2 Training

The UHE University will secure that appropriate training is in place to help employees in their day-to-day information management. All new employees must take the University's obligatory information security training to ensure that they understand the risks and their obligations while managing data. Annual refresher training will be necessary for all employees to reflect any updates or modifications in information governance best practises (Bristol University, 2018). Monitoring is an important part of an ongoing IG training programme since it allows to track and verify employee IG compliance progress

over time to ensure they are fulfilling the IG training objectives. Annually, a systematic audit, monitoring, or evaluation of the IG training program's goals and objectives should be conducted. Employee compliance with how they maintain their information according to policy directions may be addressed by conducting a post-training employee evaluation. A yearly audit process may show if staff is correctly understanding and applying policies and SOPs, and if they aren't, the audit results can be used to take remedial action until compliance improves. (Tallon, Ramirez, and Short, 2014).

7.3 Data protection monitoring

The UHE University's Data Protection Officer will keep track of new and ongoing data protection risks and update the relevant University risk register as needed, reporting to the university's management as soon as possible. The Data Protection Officer must ensure that all related policies and procedures are reviewed and updated, as well as compliance with information security incident management policies and procedures and business continuity management. The data protection officer will create and implement standards for data retention and disposal, as well as ensure that University staff and outside contractors follow the requirements. As required by law, legislation, and the University's privacy policies, the data protection officer will preserve the privacy of information (Heriot-Watt University, 2021).

8. How to Mitigate Security Vulnerabilities

In recent times, cyber security threats have increased as most universities have moved most aspects of teaching and learning online in response to the pandemic. According to Chapman (2019), in 2018 the UK Jisc security operations center (SOC) handled over 6,100 incidents and events of cyber security breaches in higher education. With this in mind, a robust cyber security framework is needed by UHE to mitigate its threats and vulnerabilities. In order for UHE to mitigate its vulnerabilities to the risk of cyber security threats, the university will implement the following:

- **Engage Stakeholders**

  UHE will engage with stakeholders which include data subjects, employees, and trusted third parties to help them understand the importance of security, their individual roles, and responsibilities, introducing them to the steps the university has taken to protect the system. According to Sapriel (2021), if organisations do not engage with stakeholders, a vacuum is created which can be detrimental to the organisation's image.

- **Install anti-Malware software**

  UHE will install anti-malware software to protect a wide range of cyber security threats including worms, viruses, spyware, and ransomware. This will protect the computers and the privacy of users. According to DHS (2015), Unprotected computers and devices ultimately form a cluster of potential high-risk infrastructure.

- **Apply patches and updates**

  Running regular updates and patches will help UHE stay ahead of cybercriminals who can take advantage of vulnerabilities in systems once it is known. A regular and frequent update will make it difficult to break into.

- **Implement Access Controls**

  With a large number of employees and students UHE has, there's an increase in the number of entry points to its network. It is essential that UHE creates access controls that will be able to limit the kind of information different users have access to. This will reduce the risk of what an attacker can access when there is a security breach.

good

9. Conclusion

In conclusion, the increase in sophistication of cyber-crime and the attack on Higher education vulnerability has necessitated the need for this document. The document would form a robust cyber security policy framework that covers all aspects of cyber security issues and will help UHE protect against a cyber security threat, adhere to professional, ethical, and legal regulations in safeguarding the confidentiality, accountability, and integrity of information.

10. Approval Table

Approval Table			
Document type	Information Governance Policy for The University of Higher Education (UHE)		
Approved by	University's Information Management Group (IMG) University Executive Board (UEB)	**Approval Date**	19/8/2021
Document version	1.0	**Next review Date**	January/ 2022
Date of publication	20/8/2021		

References

2021-22, C., 2021. Information Governance Policy Framework. [online] Imperial College London. Available at: <https://www.imperial.ac.uk/admin-services/secretariat/college-governance/charters/policies-regulations-and-codes-of-practice/policy-framework/> [Accessed 13 August 2021].

Andrew J. du Fresne. 2020. Can audits be an effective method to improve information governance compliance objectives?

Bednar, D., Henstra, D. & McBean, G., 2018. The governance of climate change adaptation: are networks to blame for the implementation deficit?. *Journal of Environmental Policy & Planning,* 21(6), pp. 702-717.

Bhaharin, S., Mokhtar, U., Sulaiman, R. and Yusof, M., 2019. Issues and Trends in Information Security Policy Compliance. 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS)

Bristol.ac.uk [online]. Available at: http://www.bristol.ac.uk/media-library/sites/secretary/documents/information-governance/information-governance-policy.pdf [Accessed 05 August 2021].

Chapman, J. How Safe Is Your Data? Cyber-Security in Higher Education. HEPI Policy Note, April 2019

DHS (2015), “National strategy to secure cyberspace, official website of the department of homeland

Hina, S. and Dominic, D., 2016. Information security policies: Investigation of compliance in universities. 2016 3rd International Conference on Computer and Information Sciences (ICCOINS)

https://www.sheffield.ac.uk/polopoly_fs/1.777636!/file/information-management-governance.pdf (Accessed: 15/7/2021)

hw.ac.uk [online]. Available at: https://www.hw.ac.uk/uk/services/information-governance/access/monitoring-evaluating-data-protection.htm [Accessed 06 August 2021].

Iannarelli, J. & O'Shaughnessy, M., 2015. *Information Governance and Security.* Oxford: Elsevier Inc. .

Ismail, W., Widyarto, S., Ahmad, R. and Ghani, K., 2017. A generic framework for information security policy development. 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)

Iso.org [online]. Available at: https://www.iso.org/standard/77802.html [Accessed 06 August 2021].

Kahn, R., 2009. *Information Nation. Seven Keys to Information Management Compliance.* 2nd. ed. Indianapolis: Wiley Publishing, Inc. .

Lomas, E., 2010. Information governance: information security and access within a UK context. *Record Management Journal,* 20(2), pp. 182 - 198.

Paul P. Tallon, Ronald V. Ramirez, James E. Short. 2014. The Information Artifact in IT Governance: Toward a Theory of Information Governance.

Ragan, C., 2013. Information Governance: It's a Duty and It's Smart Business. *Richmond Journal of Law and Technology,* 19(4).

Sapriel, Caroline. (2021). Managing stakeholder communication during a cyber crisis Vol. 4, 4 1–8 Cyber Security: A Peer-Reviewed Journal. Journal of Cyber Security and Mobility. Vol. 4. 1-8.

Smallwood, R., 2019. *Information Governance: Concepts, Strategies and Best Practices.* 2 ed. s.l.:John Wiley & Sons.

University of Sheffield (2021) Roles and responsibilities for information management governance at the University. Available at:
Yahel Ma'ayan, Abraham Carmeli. 2015. Internal Audits as a Source of Ethical Behavior, Efficiency, and Effectiveness in Work Units.

Zerlang, J., 2017. GDPR: a milestone in convergence for cyber-security and compliance. Network Security, 2017(6), pp.8-11. s

Group 3 Final copy.docx

ORIGINALITY REPORT

6%	4%	0%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of Northumbria at Newcastle Student Paper	2%
2	www.hw.ac.uk Internet Source	1%
3	Submitted to University of Wales Institute, Cardiff Student Paper	1%
4	nrl.northumbria.ac.uk Internet Source	1%
5	www.gov.uk Internet Source	<1%
6	hscbusiness.hscni.net Internet Source	<1%
7	www.fife.ac.uk Internet Source	<1%
8	"GDPR and Biobanking", Springer Science and Business Media LLC, 2021 Publication	<1%

9	bristol.ac.uk Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		

Group 3 Final copy.docx

GRADEMARK REPORT

FINAL GRADE

75/100

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

Text Comment. could also mention the word count

PAGE 3

PAGE 4

PAGE 5

Text Comment. could also discuss the related operations

PAGE 6

Text Comment. could arrange the order of the role in term of their seniority

Text Comment. who is accountable for this?

PAGE 7

PAGE 8

Text Comment. good

PAGE 9

Text Comment. could recommend some policies here

PAGE 10

PAGE 11

Strikethrough.

PAGE 12

PAGE 13

Text Comment. good

PAGE 14

PAGE 15

PAGE 16

PAGE 17

GRADING FORM: LD7087- TASK 4

AQIB AMIN	**75**

GROUP POLICY - 30%

The information security policy should include Introduction, purpose, scope, roles and responsibilities, Information Governance Policy Framework, implementation plan and monitoring mechanisms to address security threats and mitigate security vulnerabilities in the context of given scenario. Policy should include appropriate language, referencing, clarity of expression style, format and length.

Clear introduction, scope and purpose given. Good link to the frameworks and other laws. There is in **75**

depth understanding of roles, responsibilities, recommended controls, implementation and monitoring mechanism.There is an opportunity to discuss related policies in the context of given scenario. Work demonstrate academic rigor. Well done.