Information Security Policies for NewLearn

Authors:

- Võ Quang Dũng - 23199937
- Nguyễn Ngọc Phú - 23199480
- Nguyễn Huy Hoàng - 23200692

Course ID: COMP718

Course Name: Information Security Management

Date: July 3rd, 2024

Executive summary

This report offers NewLearn, a recently founded private teaching institution, a thorough examination and a set of recommendations for creating information security rules. Over 500 students are anticipated to enroll at NewLearn, and the staffing level varies from thirty to fifty. The campus computer network provides both wired and wireless access. The platforms for teaching and learning, which are available both on and off campus, are essential to the functioning of the university. Furthermore, NewLearn stores backups of the student database on a reliable cloud service provider.

To determine best practices in information security policies, our team of three experts has examined nine policy samples from three distinct colleges. We offer suggestions for the most important procedures that NewLearn should put in place to reduce information security risks based on a comprehensive risk assessment.

This report includes:

1. **Identification:** The policies that selected and the supporting information behind their selection based on our risk assessment

2. **Description:** Describe each policy using the 7 elements of an Information Security Strategic Policy (ISSP)

3. **Comparison:** Comparison of the policies to determine the best practices

4. **Outcomes:** Recommendations for the best policies for NewLearn include any necessary additions or modifications

Identification

Policies Related to Use of the Internet, the Web, and Company Networks

University, Policy, Appendix	University of Melbourne, “Acceptable Use of IT Resources Policy” **URL:** https://policy.unimelb.edu.au/MPF1314/	Stanford University, “Computer and Network Usage Policy” **URL:** https://adminguide.stanford.edu/chapter/6/policy-6-2	Stanford University, “Computer and Network Usage Policy” **URL:** https://adminguide.stanford.edu/chapter/6/policy-6-2
Note Statement of Purpose	Section 2 "Scope" outlines the purpose of the policy, defining acceptable and unacceptable use of IT resources to ensure secure and reliable services.	Section 1 "Purpose" explains the objective to promote responsible use of Stanford's IT resources.	Section 1 "Introduction" sets out the policy's aim to ensure IT facilities are used appropriately
Authorised uses	Detailed in Section 4.1 "Acceptable Use," which includes permitted activities related to academic and administrative tasks.	Detailed in Section 3 "Acceptable Use," which includes educational, research, and administrative uses.	Detailed in Section 2 "Permitted Use," which includes academic, administrative, and research activities.
Prohibited uses	Covered in Section 4.2 "Unacceptable Use," including activities like unauthorized access, harassment, and violation of copyright laws.	Covered in Section 4 "Prohibited Use," including unauthorized access, illegal activities, and misuse of resources.	Covered in Section 3 "Prohibited Use," such as unauthorized access, copyright infringement, and personal business activities.
Systems management	Discussed in Section 4.3 "IT Resource Management," highlighting the responsibilities of IT staff in managing and monitoring resources.	Discussed in Section 5 "Management of IT Resources," outlining the roles of IT administrators.	Discussed in Section 4 "IT Systems Management," focusing on the responsibilities of IT Services.
Violations of policy	Explained in Section 4.4 "Policy Violations," including potential disciplinary actions.	Explained in Section 6 "Enforcement," including the reporting and handling of violations.	Explained in Section 5 "Policy Enforcement," including disciplinary procedures.
Policy review and modification	Mentioned in Section 5 "Review," noting that the policy is reviewed annually.	Mentioned in Section 7 "Policy Review," indicating regular reviews and updates.	Mentioned in Section 6 "Review," noting the regular assessment and update of the policy.
Limitations of liability	Not explicitly included in the policy document.	Not explicitly included in the policy document.	Not explicitly included in the policy document.

Policies Related to Use of Personal Equipment on Company Networks

University, Policy, Appendix	University of Sydney , "Bring Your Own Device Policy" **URL:** https://www.sydney.edu.au/policies/showdoc.aspx?recnum=PDOC2011/140&RendNum=0	Harvard University, "Personal Device Security Policy " **URL:** https://policy.security.harvard.edu/personal-device-security	University of Toronto, "Personal Devices on Campus Network Policy" **URL:** https://www.provost.utoronto.ca/planning-policy/information-communication-technology-appropriate-use/
Note Statement of Purpose	Section 1 "Purpose" defines the policy's goal to regulate the use of personal devices on university networks.	Section 1 "Purpose" sets out the policy to ensure the security of personal devices used on Harvard's networks.	Section 1 "Purpose" explains the objective to ensure secure and appropriate use of personal devices on campus.
Authorised uses	Detailed in Section 3 "Usage Guidelines," covering permissible uses for educational and administrative purposes.	Detailed in Section 2 "Acceptable Use," which includes academic, research, and administrative uses.	Detailed in Section 2 "Acceptable Use," which includes educational, administrative, and research-related activities.
Prohibited uses	Covered in Section 4 "Prohibited Activities," including the use of insecure devices and unauthorized applications.	Covered in Section 3 "Prohibited Use," such as the installation of unapproved software and insecure configurations.	Covered in Section 3 "Prohibited Activities," such as unauthorized access, illegal activities, and personal business operations..
Systems management	Discussed in Section 4.3 "IT Resource Management," highlighting the responsibilities of IT staff in managing and monitoring resources.	Discussed in Section 4 "Management Responsibilities," outlining IT's role in supporting personal devices.	Discussed in Section 4 "Device Management," focusing on IT responsibilities and security measures.
Violations of policy	Explained in Section 6 "Non-compliance," including possible sanctions.	Explained in Section 5 "Policy Violations," including potential disciplinary actions.	Explained in Section 5 "Enforcement," including disciplinary procedures.
Policy review and modification	Mentioned in Section 7 "Review Cycle," indicating periodic reviews.	Mentioned in Section 6 "Review Process," indicating regular updates.	Mentioned in Section 6 "Review Cycle," noting regular assessments and updates.
Limitations of liability	Not explicitly included in the policy document.	Not explicitly included in the policy document.	Not explicitly included in the policy document.

Policies Related to Processing and/or Storage of Organizational Information on Non-Organizational Owned Computers

University, Policy, Appendix	University of California, Berkeley, "Data Use Agreement Policy " **URL:** https://researchdataportal.berkeley.edu/planning/data-use-agreements	Massachusetts Institute of Technology, "Information Protection Policy " **URL:** https://policies.mit.edu/policies-procedures/130-information-policies/132-policy-use-information-technology-resources	University of Cambridge, "Data Handling and Storage Policy" **URL:** https://www.data.cam.ac.uk/university-policy
Note Statement of Purpose	Section 1 "Purpose" outlines the policy to regulate the processing and storage of university data on non-university-owned devices.	Section 1 "Purpose" explains the policy's aim to protect MIT's information when processed or stored on non-MIT-owned devices.	Section 1 "Purpose" sets out the policy to ensure secure handling and storage of university data on external devices.
Authorised uses	Detailed in Section 2 "Permitted Activities," which includes academic, research, and administrative data processing.	Detailed in Section 2 "Acceptable Use," which includes research, academic, and administrative processing.	Not explicitly included in the policy document.
Prohibited uses	Covered in Section 3 "Prohibited Activities," such as storing sensitive data on unapproved devices.	Covered in Section 3 "Prohibited Use," such as unauthorized data storage and non-compliant security measures.	Covered in Section 3 "Prohibited Activities," such as storing data on non-secure devices and using unapproved storage solutions.
Systems management	Discussed in Section 4 "Data Management," focusing on responsibilities for data security and compliance.	Discussed in Section 4 "Data Management," outlining the role of IT in ensuring data security.	Discussed in Section 4 "Data Management Responsibilities," focusing on IT's role in data protection.
Violations of policy	Explained in Section 5 "Policy Violations," including reporting mechanisms and sanctions.	Explained in Section 5 "Enforcement," including possible disciplinary actions.	Explained in Section 5 "Policy Violations," including disciplinary procedures and reporting mechanisms.
Policy review and modification	Mentioned in Section 6 "Review Process," indicating regular reviews and updates.	Mentioned in Section 6 "Review Cycle," noting periodic evaluations and updates.	Mentioned in Section 6 "Review Process," indicating regular reviews and updates.
Limitations of liability	Not explicitly included in the policy document.	Not explicitly included in the policy document.	Not explicitly included in the policy document.

Description

Section	Key Elements	Purpose
Statement of Purpose	- Scope and Applicability - Definition of Technology Addressed - Responsibilities	To clearly define the policy's objectives, the technologies it covers, and the roles of those responsible for its implementation.
Authorized Uses	- User Access - Fair and Responsible Use - Protection of Privacy	To specify the permitted uses of organizational technology, emphasizing fair and responsible use, and protecting privacy.
Prohibited Uses	- Disruptive Use or Misuse - Criminal Use - Offensive or Harassing Materials - Copyrighted, Licensed, or Other Intellectual Property - Other Restrictions	To outline activities that are strictly forbidden on organizational systems, ensuring clear boundaries for acceptable behavior.
Systems Management	- Management of Stored Materials - Employer Monitoring - Virus Protection - Physical Security - Encryption	To detail the responsibilities of users and administrators in managing and securing electronic documents and data, including physical and electronic security measures.
Violations of Policy	- Procedures for Reporting Violations - Penalties for Violations	To specify the consequences of policy violations, including how to report violations and the penalties for non-compliance.
Policy Review and Modification	- Scheduled Review of Policy - Procedures for Modification	To ensure the policy remains current and effective by outlining procedures for regular reviews and potential modifications.
Limitations of Liability	- Statements of Liability - Other Disclaimers	To protect the organization from liability in cases where employees misuse company systems or engage in illegal activities, stating that the organization will not be held liable and may cooperate in prosecution.

Comparison

Scores and definitions :	
5	All ISSP policy elements present and complete
4	All ISSP policy elements present, a minor part (one or two) may need more details
3	All ISSP policy elements present, a major part (three or more) needs more details OR one or two ISSP policy elements missing but the rest are complete
2	All ISSP policy elements present but almost all need more details
1	One or two ISSP policy elements missing, some of the rest need more details
0	If none of the above applies, then the policy should get a 0 score

A score of 1 to 5 is assigned to the selected policies about "use of Internet, Web, and company networks" and provides a rationale for the score assigned

University name, policy name & location	**Score**	**Rationale**
University of California, Berkeley, "Data Use Agreement Policy " **URL:** https://researchdataportal.berkeley.edu/planning/data-use-agreements	**3.5-4**	***The University of California, Berkeley's "Data Use Agreement Policy"*** covers most ISSP elements comprehensively, including the purpose, scope, authorized uses, and prohibited uses, with clear guidelines on data management and oversight. However, it lacks specific details on the use of security mechanisms such as firewalls, IDS, and IPS, which are relevant for Internet and network use. Additionally, while the policy indicates that DUAs are subject to review and updates as necessary, it could benefit from a more structured review schedule. The policy also omits explicit limitations of liability.

		Despite these gaps, it provides detailed descriptions of authorized and prohibited uses and includes clear enforcement procedures, making it a robust framework for managing data use agreements.
Massachusetts Institute of Technology, "Information Protection Policy " **URL:** https://policies.mit.edu/policies-procedures/130-information-policies/132-policy-use-information-technology-resources	**2.5-3**	***MIT's "Information Protection Policy"*** effectively addresses the purpose, scope, authorized and prohibited uses, and enforcement procedures but lacks specific details on systems management, particularly on security mechanisms like firewalls, IDS, and IPS. Additionally, the policy does not provide information about regular reviews and updates or explicitly limit MIT's responsibility in cases of unacceptable use. Despite these omissions, it offers a robust framework for protecting information resources, ensuring compliance, and detailing authorized and prohibited uses.
University of Cambridge, "Data Handling and Storage Policy" **URL:** https://www.data.cam.ac.uk/university-policy	4	***The University of Cambridge's "Data Handling and Storage Policy"*** comprehensively addresses most ISSP elements, offering detailed guidelines for data protection and management. It clearly defines its purpose and scope, applying to all university staff, students, and associated personnel. The policy includes detailed instructions on authorized data handling, storage practices, and prohibited activities like unauthorized access and improper storage. While it discusses responsibilities related to data management and secure storage systems, it could provide more details on security mechanisms such as firewalls, IDS, and IPS. The policy outlines consequences for violations and mentions periodic reviews and updates, although a more structured review schedule would be beneficial. It does not explicitly mention limitations of liability, which is a minor omission. Despite these gaps, the policy is robust and well-structured, ensuring the protection and proper management of university data.

Stanford University, “Computer and Network Usage Policy” **URL:** https://adminguide.stanford.edu/chapter/6/policy-6-2	**4.5-5**	***Stanford University's “Computer and Network Usage Policy”*** excels in comprehensively addressing all ISSP elements with exceptional detail and clarity. It effectively articulates the purpose and scope of acceptable and prohibited uses, ensuring alignment with both academic and administrative objectives. The policy provides a thorough framework for systems management, including detailed responsibilities for IT administrators and security protocols. It includes explicit procedures for handling policy violations and outlines potential disciplinary actions, thus ensuring robust enforcement. Additionally, the policy is periodically reviewed and updated, reflecting a commitment to maintaining relevance in response to evolving technology and regulatory requirements. Although it does not explicitly address limitations of liability, the policy’s meticulous coverage of other critical aspects, coupled with its structured and comprehensive approach, positions it as exemplary in setting standards for IT resource use.

Conclusion

From the comparison, it is clear that the **Stanford University “Computer and Network Usage Policy”** is the best, scoring a 4.5-5 for its comprehensive coverage and detailed provisions across all ISSP elements. **The University of Cambridge** policies is also strong, scoring a 3.5-4, but it has minor areas that need additional details. **The University of California, Berkeley** policy scores between 3.5 and 4, indicating solid coverage with a few notable gaps. **The Massachusetts Institute of Technology** policy scores a 2.5-3, showing that it has a good foundation but lacks comprehensive details in several key areas.

Outcomes

Aspect	Similarities	Differences
Comprehensives	All policies are thorough, covering key aspects such as purpose, acceptable and prohibited uses, management responsibilities, enforcement, and review processes.	
Emphasis of Security	Strong focus on ensuring secure use of IT resources and data protection across all universities.	
Regular Reviews	Most policies mention regular reviews to keep them up-to-date.	
Specificity		The level of detail varies, with some universities providing more comprehensive guidelines and procedures than others.
Enforcement		Some policies have more detailed enforcement and disciplinary procedures.
Device Management		BYOD policies particularly emphasize device management, which is less detailed in general IT use policies.
Limitations of Liability		None of the reviewed policies explicitly include limitations of liability, which could be an area for improvement.