BUCKINGHAMSHIRE NEW UNIVERSITY
EST. 1891

School of Creative and Digital Industries

Dissertation
Academic Year 2021 to 2022

Module Title:	Project	**Module Code:**	CO707
Assignment No/Title:	Dissertation (CW2)	**Assessment Weighting:**	90%
Submission Date:	**Friday 10th May 2022 by 14:00**	**Feedback Date:**	+ 3 Weeks
Module Tutor:	Justin Luker	**Degree:**	Masters
Student ID:	**22040205**	**Student Name:**	**Harihara Shanmugam**
1st Supervisor:	**Gavin Butler**	**2nd Supervisor:**	**Nicholas Day**
Course:	MSc. Cyber Security		
Word Count:	**18055**		

Strategic Implementation of Robust Information Technology Security Policies for Higher Education

Acknowledgments

This thesis was submitted in the requirements for a Master of Science post-graduation degree program at Buckinghamshire New University through Department of Computing, School of Creative and Digital Industries. The research work described here in was conducted under the supervision of Senior Lecturer Gavin Butler, Buckinghamshire New University at the department of Computing, between January 2022 and June 2022. The thesis was written by the author who contributed to all parts of the thesis and from the initial idea to the selection of theory and research methods and from the data collection and interpretation to drafting, interviewing peoples, and revising the manuscript, equally participating to the final version of this thesis also the author paying a special greeting to Senior Lecturer Justin Luker, Department of Computing in Buckinghamshire New University also the project coordinator of this master's program for making this thesis possible. Through this opportunity making this research had opened a small window to the Information Security and get involved in Information Security community who are working in a large, international organization. This opportunity has greatly contributed to the learning and highly appreciate all the support, feedback and insightful discussions Those valuable discussions with the supervisor Gavin Butler had motivated as well as all the time devoted to the research discussions, doubt clarifications from busy schedules. Furthermore, special thanks to the interviewers participated in this research Mr Matt Hiely-Rayner Director of Strategic Planning and Change at Buckinghamshire New University and Mrs Nirosha Holton Senior Lecturer, Cybersecurity at University of Exeter for asking hard questions and for providing valuable comments on Information Security Policy and security management in higher educational institutions during the whole process and dear friend Rambabu for inspiring discussion on Information Security who pursing a doctoral programme in cybersecurity at Queens University, Belfast.

Abstract

In today’s digitally interconnected academic environment, Higher Educational Institutions (HEIs) are increasingly vulnerable to cyber threats such as phishing, ransomware, data breaches, and insider misuse. As institutions transition toward cloud-based platforms and hybrid learning environments, the need for a comprehensive, enforceable, and adaptive Information Security Policy (ISP) becomes critical. This research explores how strategic implementation of ISPs influences institutional resilience, with a particular focus on both the technical and organisational dimensions of security policy adoption in HEIs. Using a comparative case study approach, this research analyses the existing security frameworks of two major UK-based higher educational and research institutions Buckinghamshire New University and the University of Exeter—through in-depth document review and stakeholder interviews.

Semi-structured interviews with key figures from IT, security, and planning departments provide qualitative insights into how policies are interpreted, operationalised, and challenged in practice. The study further introduces a conceptual model, the “View of Reference,” which serves as a lens to evaluate how various institutional actors—ranging from policymakers to system users—perceive and engage with security policies within their organisational context.

The research investigates several technical components critical to policy implementation, including the role of Security Information and Event Management (SIEM) systems, access control mechanisms, encryption standards, endpoint security, data backup protocols, and automated incident response via SOAR platforms. Simultaneously, it assesses managerial practices such as policy review cycles, stakeholder training, ethical compliance, and the integration of frameworks like ISO/IEC 27001 and GDPR.

Key findings reveal significant discrepancies between policy documentation and real-world application, especially in areas like Bring Your Own Device (BYOD) governance, red team assessments, and incident response planning. The study highlights that security policies often fail not due to technical insufficiency but due to a lack of alignment with user understanding, institutional culture, and operational clarity.

This research contributes to the field by offering a hybridised technical-managerial model for policy deployment and suggesting an iterative, lifecycle-driven approach to maintaining effective ISPs. Ultimately, it underscores the necessity for HEIs to treat information security not merely as a compliance function but as a strategic pillar of educational resilience and public trust. The outcomes provide actionable guidance for institutions aiming to strengthen their security posture through policy-led governance, with societal benefits that include enhanced data protection, reduced service disruption, and improved digital literacy among academic stakeholders (Macnish & van der Ham, 2020; British Standard Institution, 2013; Joint Information Systems Committee, 2021).

Furthermore, the study advocates for the integration of automation and continuous monitoring tools within institutional security strategies, enabling real-time enforcement of policy rules and faster incident containment. By embedding policy logic into technical infrastructure—such as SIEM alerts, access control lists, and secure coding standards—HEIs can move beyond static documentation and achieve dynamic, responsive security postures. This work lays the groundwork for future research into adaptive policy models and AI-driven compliance mechanisms tailored to the education sector.

Table of Contents

Introduction

In the world of information security landscape, the winds of change are blowing and consistent (Cybersecurity On EU, 2022) The field has changed from being innovation, with information security being defined as a technical problem, to what world see now, with data protection being about secure management of information assets rather than technology. Classified data asset management contributes to organizational architecture, methods, protocols, and personnel. An Information Security Policy (ISP), as accepted by researchers and practitioners, is the basis for these efforts and a necessity for successful information security in an organisational environment. Building this foundation, on the other hand, is a difficult task for any business. (Alassaf and Alkhalifah, 2021) Indeed, even though firms invest large resources in developing and implementing data security rules, these policies rarely yield the expected effects. The fundamental issue is that workers seldom follow data security regulations as intended. (Alassaf and Alkhalifah, 2021) While researchers seek advice from intercontinental data security standards and best practises for designing and executing information security policies, researchers criticise this methodology for ignoring the institution's unique requirements, focusing on the presence of data protection polices rather than their subject matter, and refusing to provide guidelines on how information security policies can be constructed in practise.

A 'cut and paste' technique is unlikely to produce anything to which workers can connect or that represents the institution's broader strategy to information security. (Bhaharin, Mokhtar, Sulaiman and Yusof, 2019) While the core elements and methodologies of data protection are essential, they are just "modern architecture considerations," and attempting to define them universally does not guarantee that information security rules will be effective in any given situation. (Bhaharin, Mokhtar, Sulaiman and Yusof, 2019) As data security increasingly more of a human and corporate concern, information security policies should evolve to really include workforce and their demands. (Tang and Xie, 2010) The goal of information security policies is to impact workforce views of information security and steer them toward data protection behaviour across the enterprise. Because the ISP is a component of social realities in a certain organisation, it is vulnerable to many perspectives. If employees see the ISP differently than the corporation anticipates, the ISP will be unable to provide the products. How can the ISP represent multiple stakeholder groups' perspectives if such perceptions are unknown? Understanding these perspectives is critical since, in the end, it is the workers who establish the ISP's strength or weakness. According to this viewpoint, investigations assessing employee perspectives on different approaches applied to information security workshops, listening to each other's comments, and monitoring their activities connected to the ISP are needed. In the realm of information systems (IS), technological standards of reference have been offered to describe how to enhance workplace information security. (Tang and Xie, 2010) The standards of reference that an employee has influence how they view the security standards.

An individual's personal view of reference from a certain artefact or phenomena functions as a filter through which the antique or phenomenon is perceived and shapes one's relationship with it. The viewpoint is made up of structured knowledge about a certain information domain. As a result, it is reasonable to expect that the worker's perspective regarding the ISP contains organised knowledge about the institution's ISP; expertise that employed person has constructed upon familiarising with ISP records, engaging in problems relating to innovation adoption, utilise, and modify, and recognising employee lack of compliance with information systems. Unaligned structures of reference have been discovered to cause issues such as unaligned expectations, counterintuitive actions, opposition, and distrust, which can lead to organisational inefficacy. (Alassaf and Alkhalifah, 2021) Despite their widespread use in Information Systems (IS) research, structures of reference have not been commonly used to evaluate circumstances in the field of information security. It is also vital to clarify the structure of reference that pertains to workforce views of the ISP's involvement in information security in enterprises. Furthermore, many of the challenges related with ISP in the organisational setting like employee opposition, mistrust, lack of compliance is broadly comparable to those found by IS studies in technology advancing and suggested that most of the challenges stem from variations in the viewpoints of the core groupings to remedy this vacuum place in the research, researchers perceive a need to involves the detailed work engagement of ISP and its implications by establishing the conceptual framework of reference that pertains to enterprise Information Security Policy.

Aim and Objectives

The goal of this study is to get a greater knowledge of the effect of organizational groups views of information security policies on effective information security successful deployment in an organizational setting, expanding on the highlighted research gaps stated above. On creating the following research questions to influence the research efforts which comprises how do various organizational groups evaluate the information security policy of the organization? and what are the implications of different organizational groups' opinions of information security policies? On undertaking an interpretative instance study based on the report's goal and study objectives. The conceptual framework which develops and employ for the research report evaluation is based on the study on viewpoints and organizational information security policies. The conceptual model introduces a new idea of Information Security Policy View of Reference, which serves as researcher’s prism for studying and deeper understanding ISP perspectives and their effects. This research most widely used conceptions in information systems research may give great information for information security research, particularly a methodical technique of leadership and communication group views and their potential repercussions.

Delimitations

First section of this research outlined the study's goal and research questions. The aim of the study and Research Questions identify the critical study restrictions. Following is a full account of the constraints and the considerations that led to them.

Perceptions

The research is not engaged with how organisational ISPs are formed, constructed, or distributed (i.e., the policy application process) in organisations, but with organisational groups and their impressions of these ISPs and associated activities in a single organisation (Alassaf and Alkhalifah, 2021).

Frames of reference

The research is uninterested in how organizational groupings came to provide a frame of reference, that is, the beginnings of the viewpoints of reference. Instead, the research design is concerned with establishing the viewpoints of reference (i.e., its structure and content) that pertains to organizational ISPs, as well as the potential ramifications of those viewpoints of reference on ISP deployment and utilization.

Central Concepts

The following sections outline some of the key topics employed in this dissertation. The goal is not to offer accurate or exhaustive definitions, but to advance our knowledge of the ideas. (Alassaf and Alkhalifah, 2021) Individuals' comprehension of, beliefs about and anticipation about a certain phenomenon or item are included in viewpoints of reference (i.e., organisational ISPs). The frame of reference is used by an individual to make understanding of and attach meaning to a phenomena or item. Enterprise information security strategy on data security A group of materials used by an organisation to outline established regulations that give direction in the safeguarding of the organization's information assets is referred to as an organisational information security policy (Tang and Xie, 2010). The organisational information security policy, which is component of the institution's security practices, is focused with the organisational rather than the technical quality of information security. The organisational information security policy, which is part of the institution's information security management, is focused with the organisational rather than the technical quality of data security. Perception is a conception, image, or knowledge created by observations with a reality or thing (i.e., organisational ISP).

Risks

And an IT system is the backbone of every business. Restricting access to or interrupting this system can have major ramifications for both the organisation and its consumers (Tang and Xie, 2010). A security incident that breaches consumer information, for example, might lead to expensive in fees ranging from notification to sanctions for noncompliance with state legislation. (Alassaf and Alkhalifah, 2021) Organizations must have effective cybersecurity practises to avoid these interruptions. To provide it, they must be well-versed in two distinct areas: data security and network security. (Tang and Xie, 2010) Information security is the protection of information assets from electronic attack (Cybersecurity On EU, 2022). Network security is concerned with preventing unauthorised access to an enterprise computer systems or network. Once businesses have a firm grasp on these ideas, the next stage in developing security policy is to estimate the severity of potential attacks. (Alassaf and Alkhalifah, 2021) A risk analysis is required while developing business continuity strategies. In fact, strategic planning may be the most critical component of running any business, publicly or privately. The "criticality" (or effect) and "likeliness" (probability or possibility) of an occurrence are two basic methods for measuring risk. (Tang and Xie, 2010) This evaluation should be performed by a network security specialist who will identify what sorts of restrictions are required. These days, risk assessments can be performed by either a person or a computer. The conclusions of a risk evaluation will be used in the risk assessment to determine dangers that might harm a technology and how human factor could cause those threats to happen. All threat assessment methods begin with identifying internal weaknesses or vulnerability and external concerns, however there are several methods for being there to assess the risk management of the resources (Alassaf and Alkhalifah, 2021).

Basic Structures

The remainder of this dissertation is structured as follows. The second chapter provides a review of the literature on the relevance and purpose of security policy, difficulties related to their implementation in an organisational setting, and background on how different organisational groups may interpret them. The third chapter lays the conceptual groundwork for the investigation by addressing chosen research contributions to the understanding of viewpoints. This research expands and develops on the ideas offered in chapters two and three to establish the study's conceptual framework. The fifth chapter describes the research's methodological approach, including our reasons for choosing a single interpretative situational analysis, data collecting and analytic procedures, and criteria for performing and assessing it. The sixth chapter covers our situational analysis, including the research's setting and empirical data. The seventh chapter gives analysis in relation to the research topics and considering the research conceptual framework. Finally, the interviews are reviewed in chapter eight, followed by conclusions, some reflective views regarding the research methodology and report's shortcomings, as well as future research directions, in the final chapter.

Ethical Considerations

Testing the security of the system

To demonstrate the network security of the university network, researchers must do penetration testing or vulnerability assessments, thus there is always the question of whether revealed vulnerabilities should be exploited to install malware on systems. In certain circumstances, the researcher needs act as a hostile entity to completely evaluate the system, which may entail exploiting vulnerabilities. In such cases, the researcher may want to conduct phishing experiments, acting as a hostile entity in the methods utilized, to identify vulnerabilities. However, phishing is deceptive by nature, and it is difficult to obtain prior informed permission from study subjects for fear of jeopardizing the research. On a limited scale, limited participation study, examining without proper approval and/or using deception when the harms are minimal is typically accepted practice, such as when involved in some psychological research in which the aspect under independent inquiry is different from what the participants believe to be the case. When the process goes beyond the span of a few study volunteers, the damages become more difficult to foresee, and the absence of permission becomes more problematic. Phishing and the use of vulnerabilities to evaluate a system have the potential to inflict significant harm to people involved, which is amplified when no informed permission is given. If at all feasible, all injuries should be avoided. Where mitigation is not possible, ethical committees can assist in determining the appropriateness of the harm to the research (Macnish and van der Ham, 2020).

Responsibility

There is a continuous issue with cybersecurity in terms of the location of accountability. This is less of an issue in academic research, which is conducted under the supervision of a university with its own Research Ethics Board (REB) and hierarchical hierarchy. However, the centre of duty in commercial research is ambiguous, as is the extent to which that obligation extends. Should a firm be solely responsible for its cybersecurity development? Is this true even when the corporation is targeted by foreign nations or state-sponsored hackers? To what extent should the government assume responsibility for preserving its own market on the internet, just as it does in physical space, by establishing secure venues to trade? (Macnish and van der Ham, 2020).

Trust

Another point of concern is trust, which connects the cybersecurity practitioner to people who are supposed to be secure. There is a growing realization that security is best practiced via relationships with people who are safeguarded than imposing security on them. An antagonistic relationship here serves no one's interests, yet security is frequently despised by workers, while security staff frequently feels undervalued.

Increased openness and access to cybersecurity teams, an emphasis on increasing diversity within those teams, and initiatives by those teams to engage with the employees might be solutions to this trust (Macnish and van der Ham, 2020).

Vulnerability Disclosure

Should vulnerabilities uncovered be reported to the appropriate authorities? Such an authority might be a corporation that uses the vulnerable software, a third-party vendor of such software, or a state organization that monitors vulnerabilities. In general, public awareness of vulnerabilities is a good thing since it allows the industry to work together to determine how extensive the vulnerability is, whether any exclusive fixes have been produced, and whether the issue has been leveraged. But there is a danger that by publishing the vulnerability, throughout a small group of cybersecurity specialists, knowledge of the issue will leak and be leveraged. Despite the research on the importance and necessity of vulnerability disclosure, during research awareness about the just a few universities (REB) that have a vulnerability disclosure policy. Vulnerabilities are expected to be uncovered during cybersecurity research, maybe even more than incidental finds, and it is critical that individuals managing that study have clear guidelines on what should occur in those cases. A vulnerability disclosure strategy would also safeguard the researcher in circumstances when vulnerabilities are found but no informed consent was sought, which might be difficult to acquire. In such circumstances, the harmed party is quite likely to sue the institution or researcher. Is there still a responsibility to publicize such discoveries in such cases? How much risk should each researcher and research organization bear in exploring such dangerous vulnerabilities? The replies will differ depending on the university, but clarity is crucial once again to safeguard the researcher (Macnish and van der Ham, 2020).

Business ethics

Business ethics, and the conflicts that develop because of opposing goals in security and producing money, Security should not be overlooked to transfer funds into revenue operations, and a small amount of foresight will imply that strong security will increase a company's reputation and users with reliable in that institution. Nonetheless, it would be wrong to think that there are no conflicting interests between personal interests, public interests, and organizational objectives. Certain top executives sold their shares in the firm only days before the 2017 Equifax hack was made public (Macnish and van der Ham, 2020).

Respect for persons

Participation as a significant subject to be investigated is entirely voluntary and accompanied by informed consent. Individuals should be considered independent agents with the ability to choose their own identities. Individuals who are not research subjects but are affected should be treated with respect and dignity. Individuals with diminished independence are protected, as are those who are unable to take on more responsibility (Macnish and van der Ham, 2020).

Informed Consent

Informed consent is the cornerstone of ethical research. The phrase consists of two crucial parts, 'informed' and 'consent,' both of which require careful study. Participants must be properly aware of what is expected of them, how the data will be utilized, and what, if any, repercussions may result.

To participate in the research, individuals must offer clear, active, written consent, indicating recognizing their rights to access their information and the ability to withdraw at any time. The procedure of informed consent may be viewed as an agreement between the researcher and the participants. Information will be analysed and reported, and what are the dangers of participating in the study? information on the right to withdraw at any time for any reason (including removing previously provided data), security guarantees that participant authenticity will be kept private, clarity on data protection (participants own their original data, researchers own the statistical results), and their right to access their data, the right to demand additional information, and data on the dispute settlement system (contact details of the researcher along with a supervisor, or the research ethics committee). It is critical that the provided specific permission form be strong, clear, and properly written. What level of dedication is expected of participants? If the official document and consent form are confusing, it will result in a poor involvement in decision making, which may jeopardize the quality of data obtained due to distrust and will not guarantee appropriate safeguards for the participant or the researcher (risk of harm) (Macnish and van der Ham, 2020).

Anonymity and Confidentiality

It is critical that participants' identities be kept secure or unidentified, and the assurances go beyond preserving their names to include the prohibition of utilizing of the self-identifying remarks and material. Anonymity and secrecy are critical steps in safeguarding people from danger. Participant identity and participant privacy are two phrases that are sometimes used interchangeably when they are not. Participant confidentiality means that the researcher is unaware of the participant's identity (e.g., when using anonymous surveys, the participant's information is truly hidden from the researchers). The confidentiality of participant data refers to data that is de-identified and the participant's identity is kept private. Usually, this only applies to interviews, which are conducted knowing the participant's identity, therefore anonymity cannot be offered. The research design needs to consider the potential of harm to the participants, the researcher, scientists, the wider community, and the research institution (Macnish and van der Ham, 2020).

There can be the harm in the form of physical injury, resource loss (including time), emotional pain, and reputation damage. The first step is to eliminate, isolate, and minimize the potential harm. In addition, the committee should ensure that participants are fully informed of the potential conflicts of interest that could arise within the research project, so the committee can provide guidelines on how to manage them and it is critical to disclose on this conflict of interest publicly within an ethical approval application so that the committee can give advice on how to handle it.

It is usual for researchers to undertake research in conjunction with their institutional programmes, where the researcher may also have instructional (and assessment) duties as well as line supervision of study participants (Macnish and van der Ham, 2020). The remedy to a power differential conflict of interest is to remove the cause of the power disparity. For example, a lecturer abstains from becoming an assessor of the student participants' work, data collecting is performed by a private entity who de-identifies the information before making it accessible to the researcher, or data gathering is confidential (e.g., anonymous surveys) to guarantee that the teacher is unaware of the participant's identification. Likewise, it is unusual for researchers to have commercial interests, and these actions may have an influence on research involving partners with comparable commercial interests (Macnish and van der Ham, 2020).

Literature Review

Security Policy

A security policy is a document that outlines how a corporation intends to safeguard its physical and information technology (IT) assets. Security policies are dynamic documents that are constantly updated and modified as technology, vulnerabilities, and security needs evolve (What is an IT Security Policy? 2022). An acceptable usage policy may be included in a company's security policy. These indicate how the organization intends to educate its staff about asset protection. They also include a description of how security measures will be implemented and enforced, as well as a method for reviewing the policy's efficacy to ensure that required adjustments are made (Importance of acceptable use policy – IT Systems & Services | Bio Melbourne Network, 2022). Security policies are crucial because they protect an organization's physical and digital assets. They identify all the company's assets as well as any risks to those assets (What is an IT Security Policy? 2022).

Making Good Security Policy

A solid security policy is made up of various components. The most critical aspect is that it is useful. A security policy is useless to an organization or its employees if the principles or requirements outlined in the policy are not followed. To give the information required to apply the legislation, it should be brief, clearly stated, and as thorough as feasible (IBM Docs, 2022). It should be updated to the latest and dated so that the most recent document is easily recognized, and it should be internally organized such that important or needed material is recognized and easily accessible within the record for reference. A strong security policy also considers current or implicit regulations in use. Organizational business processes change over time as employees discover more effective ways of interpreting data. A security policy should not inhibit or interfere with company operations.

Rather, it should improve the process by instilling trust in the security of the everyday routine core activities. A security policy should constantly consider the interests of workers, third parties, and the company's commercial goals (Adrian Duigan, 2022). For example, security rules that provide for the privacy of information and details consider the sensitivity and necessity of protecting their staff. It is also crucial to consider securing the assets of any alliance partners. When developing a security policy, have draughts evaluated by representatives from several departments, including IT managers, legal and human resources workers, and executives. This will result in a document that represents and answers the needs of all stakeholders inside the company (How to create an effective security policy: 6 tips, 2022).

Security policies can impact purchasing decisions since goods must address security as defined in the policy. As a result, a robust security strategy will aid in the development of regulations for software, hardware, and other network equipment. Security policies will also assist in determining what steps should be performed and who should be alerted in various scenarios. This helps to urge consumers to act sooner, thereby preventing or lessening the consequences of any data security breaches (How to Create a Good Security Policy, 2022). The policy should also specify what corrective activities should be done following a breach, as well as any legislative or criminal consequences that may be imposed circumstances. Well, inclusive security policies will always aid in offering direction and instructions for policies in other sectors.

Privacy should be treated not only by security, but also by legislative, human resources, and administration. Finally, because a security policy is a living document, it must be re-evaluated on a regular and controlled basis to ensure that it is updated and addresses all pertinent scenarios, settings, and systems inside the business. (IBM Docs, 2022).

Categories of Security Policy

A security policy has several components; however, they are generally divided into three groups. The first category describes the characteristics utilized in the policy. This section may contain several subsections. The second portion generally describes a risk assessment or certification procedure, and the last section contains the rules and recommendations derived from the second section. (ISP Templates | SANS Institute, 2022).

Introduction

Typically, the introduction at the start of the paper outlines why and how the security policy is being adopted by the institution. Essentially, this is an explanation of the purpose the policy was formed, an explanation of the stakeholders who established the policy and describes the contents of the policy handles in it (ISP Templates | SANS Institute, 2022).

Audience

The second half of the characteristics section covers the policy's target audience, which is typically the broad populace of an organization, including normal users, IT employees, managers, and so on, and together with whom it is designed for, and the target section specifies which main aspects of the security policy structure apply to each target audience group (ISP Templates | SANS Institute, 2022).

Definitions

To guarantee that anyone who reads the security policy has the same knowledge of the specified standards and procedures, it is critical to include a description of the terminology used within the policy. This prevents any misconceptions, inadvertent mischaracterizations, or absence of clear comprehension due to a lack of knowledge of words used within scope of the policy (ISP Templates | SANS Institute, 2022).

Physical security

Physical security rules are designed to safeguard an institution's physical assets, such as infrastructure and facilities, such as computers and other IT facilities. Data security rules safeguard intellectual property from expensive incidents such as security breaches and data leakage (Irwin, 2022). Physical security rules safeguard an organization's physical assets, which include buildings, cars, inventories, and machinery. IT equipment such as servers, computers, and hard drives are examples of this assets.IT physical asset protection is very critical since physical equipment carries firm data. If a physical IT infrastructure is compromised, the data it stores and manages is endangered. To keep firm data safe, information security policies rely on physical security standards. As part of a physical security policy, companies identify sensitive areas in their buildings, rooms, and other areas of the organization, establish procedures for accessing, monitoring, and handling the assets, and state who is responsible for which assets.

Physical security policies also specify how employees are responsible for the assets they access and handle (Irwin, 2022). Physical assets are protected by security guards, front entry gates, and locks on doors and windows. Physical assets can also be protected using high-tech methods. An access control system based on biometrics, for example, can help limit access to a server room. The fingerprint scanner would be used in the room to determine if a person entry is authorized (Irwin, 2022).

Information Security

Information is the most asset of any organisation; therefore, information security is the major component to be considered on making the security policy of an organisation, which elaborates the current information security status in a specific organisation.

Subsequently, a brief analysis of risk is to be performed with help of threat intelligence of a specific industry such as Higher Educational Institution, Information Technology companies, Government firms, Aviation, and Heath etc. People who are more integrated with the environment of organisation should be participated in the study of risk analysis. Information gathered by risk analysis is fundamental asset of the organisation, so they are stored confidential and accessible to strictly to authorised people only (Cisco, 2022).

Information security policies

These policies provide the following advantages like protecting valuable assets. In general data integrity, confidentiality, and availability are known as the CIA Triad is protected by these policies (F5 Networks, 2022). Personal information and sensitive customer data are typically protected by these policies. An organization's reputation can be negatively affected by data breaches and other IT security incidents. Ensuring the organisation security posture is maintained under and meets compliance with legal and regulatory requirements. (Smith, 2022) Many regulatory provisions, legal compliances, and laws target sensitive information (FSB, 2022).

The Payment Card Industry Data Security Standard, for example, governs how businesses handle customer payment card information. The Health Insurance Portability and Accountability Act specify how businesses should handle protected health information. The organisation security policy provides guidelines for protecting data and intellectual property. Violations of these rules can be expensive. Information generated by every employee poses a security risk. The focus should focus on third-party vulnerabilities are also needed to consider because third party organizations might have different security standards, so some vulnerability may arise as a result.

These gaps are identified by security policies. When designing security rules, enterprises must examine how they use the cloud and mobile apps. The data stored cloud computing and mobile devices are also to be secured (FSB, 2022). Data is rapidly being dispersed across a variety of devices via an organization's network. It is critical to account for the increasing number of vulnerabilities introduced by a dispersed network of devices. Data categorization of these data and information is also vital. Improper data categorization might expose valuable assets or waste resources safeguarding data that does not need to be safeguarded. It is very important that to monitor the cyber assets and updates of system and to fix the patches through these updates. The IT infrastructure of a company and the risks to which it is exposed vary as the company expands, industries change, and cyber threats adapt. To reflect these developments, security rules must evolve. The policy framework structures are to meets the industry standards. The National Institute of Standards and Technology (NIST) publish a Cybersecurity Framework that gives recommendations for organisations and these frameworks helps to structure the organisational security posture to detect, prevent and response to the cyber threats (NIST, 2022).

Secure System Architecture in Policy Enforcement

Beyond documentation, effective information security in Higher Education Institutions (HEIs) depends on embedding security policies into the technical architecture of the organisation. This includes implementing network segmentation, access control lists (ACLs), secure endpoint configurations, firewall zones, and role-based access.

For instance, if a university policy prohibits access to torrenting websites on campus, the firewall should be configured accordingly to block such traffic. Moreover, authentication policies must align with technical controls like Single Sign-On (SSO), Multi-Factor Authentication (MFA), and secure password hashing algorithms. The use of secure APIs, TLS encryption, and regular patching workflows must also reflect what is defined in policy documentation. By integrating policy rules with system architecture, institutions can ensure enforceability and reduce reliance on user behaviour alone. This architecture-policy alignment is essential for building resilience and achieving measurable compliance outcomes.

CIA Model

Confidentiality: The efforts of an organisation to keep its data private or hidden are referred to as confidentiality. In practice organization, it means restricting data access to avoid illegal disclosure. Typically, this entails ensuring that only authorised individuals have access to specified assets and that unauthorised individuals are actively prevented from gaining access. Only approved Payroll personnel, for example, should have access to the employee payroll database.

Confidentiality may be breached in a variety of ways, including direct assaults aimed at gaining unauthorized access to systems, applications, and databases to steal or manipulate data. Monitor or scout an attacker's network as well as other forms of system scanning, eavesdropping, and privilege escalation (F5 Networks, 2022).

Integrity: In common parlance, integrity refers to the property of being full or whole. Integrity in information security refers to ensuring that information has not been manipulated and can thus be trusted. It is correct, authentic, and trustworthy. Customers who shop online, for example, demand accurate product and price information, as well as the assurance that quantity, pricing, availability, and other information will not be changed after they make an order. Customers must have confidence that their banking information and account balances have not really been manipulated data integrity entails safeguarding data while it is in use, in transit, and when it is stored, whether on a laptop, a portable computing device, at a data centre, or in the cloud. Encryption, hashing, digital signatures, and digital certificates are examples of data integrity safeguards. Trusted certificate authorities (CAs) provide digital certificates to companies to verify their identification with website visitors, like how a passport or driver's license may be used to validate an individual's identity.

Systems, programmes, and data are worthless to a third-party organisation, customers, and its stakeholders if they are not available when authorised users require them. The description is clearly directed to the availability of networks, systems, and applications. It guarantees that authorized users have quick and dependable control over resources when they are required (F5 Networks, 2022).

Availability: The availability of services can be compromised by a variety of factors, such as hardware or software failures, power outages, or natural disasters. Denial-of-service attacks are often well-known threats to availability because they degrade a system's or website's performance or cause the system to be unavailable (F5 Networks, 2022).

One of these three principles might take precedence over the others, depending on the security goals, industry, and business nature of an organization. One of the most important to apply CIA triad concepts is that assessing priorities can mean compromising others. Systems that require high levels of confidentiality and integrity, for example, might sacrifice lightning-fast performance that other systems value more. Trade-offs isn’t always bad things; they're intentional decisions. These principles must be applied according to each organization's unique requirements, while also balancing the desire to provide seamless and safe user’s experiences (F5 Networks, 2022).

ISO Standards

The worldwide standard for information security is ISO/IEC 27001:2013 (commonly known as ISO 27001). It specifies the requirements for an Information Security Management System (ISMS). The correct approach of ISO 27001 assists businesses in managing their information security by making communication, processes, and technology. Certification to the ISO 27001 Standard is recognized globally as proof of Information Security Management System (ISMS) is in line with best practices in information security (ISO Governance, 2022). The ISO 27001 is a framework that assists businesses in establishing, implementing, operating, monitoring, reviewing, maintaining, and constantly improving an Information Security Management System (ISMS). It is part of the ISO 27000 set of information security standards. An information security management system (ISMS) is a comprehensive strategy to ensure the confidentiality, integrity, and availability (CIA) of business information resources. Policies, procedures, and other constraints involving people, processes, and technology comprise an ISO 27001 ISMS.

An Information Security Management System (ISMS) is an effective, risk-based, and technology-neutral strategy to secure university information assets that are informed by frequent information security risk assessments. The ISO 27001 toolkit contains all the pre-written policies, regulations, and templates that helping stakeholders who need to develop an ISO 27001 information security management system (ISO Governance, 2022).

Access Controls

Access entails far more than simply entering the facilities. Access to critical or otherwise sensitive documents, files, directories, proprietary information, or systems is also a major component of access restrictions. The procedures for approving access to systems and information, as well as those for terminating employees, should be outlined here. Remember to include staff remote access, internet connections for other organizations, and public location access (Sailpoint, 2022).

Authentication

Authentication is the process of determining if a person is who they say they are and whether they have the necessary credentials to access locations. The authentication mechanism should be specified, whether it be basic password challenges, two-tiered authentication systems, or the more complex biometrics now in use. Include the criteria that regulate them in the standards, such as how many authentications tries are authorized before shutting access, and how strong the specific technique used should be for example, the length and characters included in a password define how secure it is organized (OAuth, 2022).

Encryption

The act of transforming plain and legible material into undecipherable methods to secure and manages privacy is called as encryption and it has become a widely used technology. It is used to establish digital signatures that authenticate user identity and to safeguard data that goes across public networks, like e-mail. Standard regulations must be specified, and the setup used described to avoid lack of accessibility and uncertainty over what sort of encryption to use to encrypt the files (Norton, 2022).

Backups and Recovery

The Importance of Backing Up

Even though university got the good infrastructure and facilities, but the university laboratory computing systems or external hard drive is, they will eventually fail. That's just the way any piece of hardware or software works. Repair companies which provide services to the university computing system might be able to extract the data, but they might not. (Backups, 2022) That is the risk institutions take when they do not back up their data.

Worse, there are several dangers to the integrity of academic data on the Internet. Viruses and Trojans do more than merely steal data from universities. They vanish in some circumstances. (Backups, 2022) Ransomware attacks are also becoming more prevalent. A hacker installs a virus on a university computer that encrypts university information. The institution must then spend hundreds of dollars to obtain decrypted university data. This is less of a problem if the university has backed up its data.

The institution can simply erase the hard discs and restore from the most recent backup. It makes little difference if an institution loses data due to technical failure, a natural calamity, or criminal intent; the data is gone. The information, nevertheless, does not have to be lost (Backups, 2022). It also highly supported by the Higher education institution.

How to Back up University Data

There are several methods for backing up educational data. Each will have its own set of processes. Still, there are certain fundamental rules to follow while creating a reliable backup. Storage is now so inexpensive that simply backing up everything makes perfect sense. University may be capable to save a few cents by just keeping items that cannot be replaced. Most current computer users, on the other hand, will also want to back up all the information merely because it is inexpensive to do so. Cloud storage has several advantages over local storage. (Plesk, 2022) For example, if the university home is flooded, the backup would most likely be lost unless the institution has it saved in the cloud. It is better to store a data of the organization in a multiple location. Do not even feel obligated to choose between a local database traditional backup and cloud backup. Institution's best bet is to back up both.

Similarly, maintaining tangible copies of items like educational institution bank statements and tax documents is important. It is advisable to preserve a physical file of the institution's most significant documents, in additional to whatever backups the university has. Determine what the university needs to back up. The documents are going to be the most important part of university backup. Take some time to organize university documents if they aren’t already. That’s going to make it easier to ensure that university backed up everything that university need to backup.

For example, some of university applications might be stored in the cloud whether university realizes it or not. Some university applications, for example, may be saved on the cloud whether the university staff is aware of it or not. Documents will be the most crucial aspect of institutional backup. (Plesk, 2022) If you haven't already, arrange your university paperwork. This will make it easy to guarantee that the institution has backed up all that it has to. Considering data changes on a regular basis, application data is one of the more challenging things to backup. If the institution depends heavily on apps, it may want a backup strategy that backs up routinely – daily or more – without the institution having to instruct it to. Whenever the institution purchased the operating system, it most likely came with a backup. However, keep in mind that if the institution ever must reload the backup, most of the academic environments would be gone. Backing up is not an all-or-nothing proposition.

It's a great way to keep a couple of external drives on available for backing up recent vital documents. Again, university requires as many levels of backup as possible. The likelihood of losing all university data in a calamity is low, yet it is larger than zero. Backup is unquestionably one of those "effectively cautious than sorry" items. It is cheap and easy to do, but the penalty of not doing it might be a lifelong of regret (Plesk, 2022).

Risk Assessment

A risk assessment of resources performs several functions. The most apparent and significant purpose of a risk assessment is to quantify the risk involved with the systems. Applying protection to an organization's assets has a cost, expenditure on security tools, appliances, and apps. A system inventory is typically undertaken in combination with a risk assessment. (CHAS, 2022) A risk assessment will evaluate whether dangers exist for an organization's systems and how severe the risks are for those assets. The findings will aid in prioritizing systems from the most dangerous to those with the least exposure and risks. This will assist in determining which places require the greatest level of security and how those areas should be secured. The aims of asset security are to offer the highest levels of availability, integrity, and confidentiality, and a risk assessment must always analyze threats and vulnerabilities in terms of how they will influence these three aspects. (CHAS, 2022).

Quantitative Risk Assessment

Quantitative risk assessment uses financial metrics to analyses risk. It uses mathematical formulae to calculate the number of projected losses associated with a certain risk, depending on the valve of total assets, frequency of risk occurrence, and likelihood of loss (CHAS, 2022).

A quantitative evaluation of fail over would include evaluating at the expense of a server or the income it generates, how frequently the server crashes, and the projected loss caused each time it failed. Researchers can derive various important computations from these data. Single loss expectancy is the expenses that the researcher would suffer if the incident occurred just once per year annual rate of recurrence however many times per year the researcher can anticipate this hazard to occur yearly loss expectancy is the overall risk value over the period of a year (CHAS, 2022). These quantitative results may aid researchers in avoiding wasting time & expense on lowering insignificant hazards. For instance, if a danger is relatively uncommon or involves expenses are very little to mitigate, it is considered to pose a limited risk to stakeholder businesses. But, whenever a danger to an institution's critical IT infrastructure is likely to occur and might be costly to repair, or if it is likely to negatively impact stakeholder business, future studies should consider it risk factor. Institutions may wish to utilize this risk information to perform an economic feasibility analysis to assess what degree of expenditure would be beneficial for risk mitigation strategies. Consider that quantitative risk metrics are only useful when stakeholders have access to accurate data. Because IT-related threats and risks can fluctuate wildly, stakeholders don't always have the requisite statistical information to calculate likelihood and expense estimations (CHAS, 2022).

Qualitative Risk Assessment

It is just subjective assessment of resources or based on opinions. It depends heavily on judgment to categorize risks based on likelihood and consequences, and it employs a rating scale to describe the potential dangers as follows as low - unlikely to take place or influences stakeholder business like in medium is likely to happen and impact high is likely to happen and severely influence stakeholder business For instance, this evaluation may be classified as high likelihood since there is something that researchers may anticipate to occur multiple times every year (CHAS, 2022).. The researcher may do the similar for cost effect in whichever parameters appear relevant, for example, low would result in a reduction of up to half an hour of output, medium would result in a total and complete suspension for at least four days, and high might result in an irreversible loss to the firm. After determining customer ratings, researchers can develop a risk assessment framework approach. To assist stakeholders in categorizing the risk level associated with each risk occurrence. This can eventually assist stakeholders in deciding which risks to mitigate through controls and which to tolerate or transmit (CHAS, 2022).

Threats to Information Security

In Higher Educational Institution contains massive amount of data and information of students, employees, and faculties also their data regarding academic work and research work which is meant to be classified and this data and information easily attracts the minds and interest of the hackers worldwide.(Toptal, 2022) The large number of students on daily basis connecting their own personnel devices to the institutional network had creates the possible easy routes to bypass or penetrate the organisational network due to this functional transparency the network of higher educational institution had become very easy target for the hackers. Complete prevention of cyber-attacks is not possible but necessary robust procedures and protocols should be followed to maintain the confidentiality, integrity, and availability of the information also to govern the reputation of the university (Toptal, 2022).

Cyber related training to employees which Information Technology security and Data protection laws and compliances like GDPR (General Data Protection Regulation) and they should be aware of fundamental knowledge of cybersecurity on both technical and organisational measures and their impacts on higher educational institutions.

These measures ensure the degradation of the chances of the hackers to penetrate the network or compromise the system completely, so thereby can prevent the occurrence of major hack of an organisation from the intruders. These are factors to be considered by executive officials like CISO (Chief Information Technology Officer) who is responsible for overall security posture of an organisation. (CISO, 2022)

Types of Threats

Ransomware

Definition: A special malware type attack launched out by hackers that leads to data encryption of the data files stored in the computing system and the massive amount of ransom is demanded by hackers to provide a digital key to decrypt the encrypted data stored on the devices and it has evolved into serious threat worldwide to every industry.

In the past Government organisations, Health care, and Critical Infrastructure are the curious targets of these types of attacks, but at present higher educational institutions are their most intended targets and cyber-attacks towards them had rapidly increased. (Ransomware, 2022)

Case studies:

Even during COVID-19 crisis, there was a wave of cyber-attacks targeting schools, universities, and institutions. These include destructive security breaches on two other universities in the North-East of England last year, as well as universities such as Newcastle University and Northumbria University in April 2021, and few other organisations such as the University of Sheffield and the University of Portsmouth, which experienced network shutdowns enduring days after ransomware malicious actors struck (UK Universities, 2022). Following the pandemic's digital transformation initiatives, especially the transition to open and distance learning, it appears that hackers see this industry as an easy target. Following a wave of assaults on the higher education, the UK's National Cyber Security Centre (NCSC) revised its ransomware warning in July. (NCSC, 2022). Lincoln College, the most extreme case of a school afflicted by ransomware, was forced to lock its doors permanently on May 13 after 157 years of existence. The COVID-19 epidemic originally hampered the school's capacity to recruit and finance for the private organisation. (NCSC, 2022) However, the ultimate failure shift occurs when the college struggled with a catastrophic December ransomware assault that hindered staff access to critical school data, making it even harder for the school to discover new potential students and so reducing the institution's capacity to keep its gates unlocked. Every technology essential for recruiting, retention, and financing initiatives were dysfunctional is the statement proposed according to a post on the Lincoln College website. Thankfully, no personally identifiable information was disclosed. (UK Universities, 2022).

SQL Injections

The SQL (Structured Query Language) based injection attacks or insert of malicious modification of input data into the application. SQL injections can lead to the extraction of classified data from the database, data modification in the database and further privilege escalation of administrative functions in the database includes shutting the of DBMS (Database Management System) process or data recovery of the contents of the specific file in the DBMS file system (OWASP, 2022).

Issuing commands to applications and operating systems are usual way of approach of these types of attacks. These applications consist of varied classified information from student academic work to researcher paper works, therefore if continuation of weakness in databases will always keep the higher educational institutions in the dark side of hacking. An effective utilization of strong password policy to the protected online application should be used by colleges and students. (Slip, 2022)

Phishing

This type of attacks is characterized by spamming of users to reveal their classified data such as information related to credit cards, usernames and passwords through entering these credentials in the malicious web pages or emails which is specifically tailored to perform these kinds of attacks. (Phishing, 2022) The Implementation of industry standard antivirus software, cyber hygiene practice and anti-phishing filters will reduce the chances of hacker's phishing campaign.

A Business email accounts takeover has frequently occurred and at present it is the one of the major threats to the higher educational institutions. The email accounts are compromised in these techniques and stolen of account credentials. The email spams and phishing attempts are propagated in thousands to all staffs and students in the organisations through the hacked email accounts with help of stolen credentials. (Phishing, 2022)

Data Protection

Awareness of data protection is biggest challenge in higher educational institution and educating their workforce about the changes GDPR will bring is very important. People in academics, management, deans, vice-chancellors, and other university officials need to be developing awareness of the implications of the changes to data protection legislation. (Search data, 2022) Information security auditing is more crucial to every organisation to analyse the procedures involved in protecting the cyber assets of the company. There will be a greater emphasis on accountability for the data held by institutions. GDPR requires organizations to keep records about the personal data they collect, how they collect it when it will be deleted, and who has access to it, in addition to keeping records about what personal data is stored within their organization systems. From phone records to employment information, this data will be collected. Massive amounts of sensitive and non-sensitive information will have to be classified, and all this information subjected to be in private and mapped.

In Information Security Incident response is very important to every institution to solve the problems and recover back their services. (Search data, 2022) The classified information must be kept protected and the Information Commissioner's Office (ICO) will be required to be informed within 72 hours if there has been a security breach that poses a risk to the individual. The situation might arise, for instance, in the event of financial loss or in cases of identity theft, and organizations should also notify the individuals involved.

A critical element of this process is incident response, which describes the procedures for detecting, investigating, and responding to data breaches. Every organisation should design their design university of data protection and in some cases, institutions do not need specific, informed, and unambiguous consent for data processing, but where they do, they must be able to demonstrate that the consent was freely given. Rather than simply failing to opt-out, individuals will need to explicitly operate in. Continuing with the concept of consent, institutions will be required to consider whether the collection of data and its processing is necessary. Recognized legal bases include contract, legal obligation, vital interest, public interest or legitimate interest of the organization. If these apply, then processes must meet the requirements of GDPR.Institutions will be required to examine whether the collection and processing of data are necessary about consent. (ICO, 2022) Legal bases recognized by law include contracts, legal obligations, important interests, government interests, or legitimate public opinions and interests of the organization. When these factors are said to be apply, then GDPR requirements must be followed to the protection of data. Individual rights must be informed when accessing their personal data, including the legal basis that is used to process their data, as well as the data retention period, and their right to lodge a complaint with the ICO. The notice will typically take the form of a privacy statement. (ICO, 2022)

Need of Information Security Teaming

The misinterpretation of IT (Information Technology) teams and IT Security teams had been a biggest setback for maintaining the security posture of every company. As fundamental IT teams are responsible to the functional capabilities of IT assets and IT security teams are responsible for to maintain security posture of IT assets of an organisations. (Rapid 7, 2022) The security and functionality of IT is always not maintained in a stable equilibrium, but organisation is to be some flexible towards to security because information is the most valuable assets of every organisation.

The shortage of information security employees and the absence of executive positioning executive officials like CISO (Chief Information Security Officer) in universities has become greatest threat to higher educational institutions. The lack of investment in cybersecurity strategies, educating awareness about cyber hygiene to students and employees and maintaining the security posture of resources effectively had led to weakness to the posture of organisation.

The inadequate manpower in the number of staffs and lack of knowledge of employees how to tackle cyber challenges in this cyber era and prepare themselves to develop cyber resilience to protect the assets and respond to the incidents occurs in the organisation to protect the confidentiality, integrity, and availability of the information also to govern the reputation of the higher educational institutions (Rapid 7, 2022).

Asset Management

IT asset management is the process of ensuring an organization's assets are accounted for, deployed, maintained, upgraded, and disposed of when the time comes. Put simply, it's making sure that the valuable items, tangible and intangible, in university organization are tracked and being used. The IT asset includes hardware, software systems, or information an organization value. In IT department, some of our most important assets are the computers and software licenses that help us build, sell, and support all software and the servers hosted in this research. Asset management keeps information updated, so teams eliminate waste and improve utilization. It saves money by helping avoid unnecessary purchases and cutting licensing and support costs (IT Asset, 2022).

To strengthen security policy enforcement, asset management systems should be integrated with endpoint detection tools and automated inventory tracking. Solutions like agent-based asset monitoring and configuration management databases (CMDBs) allow IT administrators to detect unregistered or non-compliant devices accessing university networks. This integration ensures that policies—such as software version control, patch management, and license compliance—are automatically enforced and aligned with the institution's overall robust cybersecurity posture.

Shift to Remote Learning:

Due to pandemic lockdowns had increased work from home and remote learning technologies to maintain learning continuity. To enhance educational experience academic modules through internet even through video streaming and portable computing devices thereby schools, universities are likely facing serious cyber threat from hackers worldwide because sudden shift to modernised process of remote learning both students and faculties are need to usage of their personal computing devices so there is no verified security posture of their devices which they are using to connect to the organisation network therefore the data stored in those computing devices and organisation network are subjected to be desired asset to hackers worldwide. Due to insecure internet connection and lack of personnel device protection like anti malware security these devices are exposure to variable vulnerable postures these devices are exploited by cyber based attacks like phishing, data breaches, ransomware and SQL injection etc. (Blog, 2022)

Academic Integrity

Academic integrity is the personal integrity owned by the institution and holds the reputation of the organisation because it reflects the own work generation to uplift the university ability to produce best graduates to the society. This reveals university earned the recognition and potential to the preparedness for the changes and to withstand the position to tackle the challenges in higher education profession that needs to solve in future.

Academic integrity is the main promotion of every higher educational institution, so student education is about academic integrity of the organisation so when academic misconduct occurs universities are responsible for taking necessary steps to safeguards its integrity and reputation. (AMT, 2022) Prevention of academic misconduct can be achieved through procedures and this misconduct is managed and controlled by university management also it is responsible to safeguards the standard of academics in the university and ensure that university providing genuine awards and credits to the work they are produced under their own research which they are submitted for evolution. This allows university to protect the student interest that is very genuine on their work and satisfies the obligation standards of reporting and meeting the high educational provider rules and compliances. Employers generally recognise the student performance and standards by their degrees awarded to them which satisfy the criteria of standard educational program and professional qualifications. Most of the demanded jobs in the market need the bachelor's degree qualification because professional ethics, industry standards and behaviours exist and accepted in many professions. (Arkansas, 2022) The Employee trustworthiness, ethical moral valves and responsible behaviours are mostly expected and accepted by the employers, therefore adoption of integrated procedures to safeguard the academic integrity and in posture to address the academic misconduct of students which involves plagiarism, malpractice, essay mills, collusion and cheating or faculties academic misconduct involves partiality in evolution is needed for higher educational institutions (Arkansas, 2022).

Business Continuity and Disaster Recovery

Detailed information and additional guidance to the steps needed for restoration of critical operations of the university must be the section of business continuity plan. A business continuity plan in general focuses the protection and ability of the universities to recover from the disasters and to develop the secure posture to maintain resilience for long term can be achieved only through organising and consistent reviewing the plan and incorporates mandatory updates (Azeus, 2022). During business board meeting the business continuity plan should be given more importance to discuss about its growth and functionality. (Business Continuity, 2022) Like Information Technology companies, nowadays higher educational institution is also put a great deal on drafting their own business continuity plan to provide customer services which include students and faculties depends on. In additional to financial loss and dissatisfaction on the academics and student experience is may cause serious setback to their enrolment. (Business Continuity, 2022)The poor employment opportunities after graduation and disability to plan for long term goals in future is also leads to disengagement of their courses and gives negative feedback to the universities among the students, therefore these problems will reflect future enrolment of students, talent employment of faculties and also affects the reputation image of the organisation so it act as barrier to attraction of investors to the organisation and effective enrolment of students is necessary for every higher educational institution because student tuition fees is the major revenue in their financial assets (Azeus, 2022).

Methodology

Comparative Analysis

A prominent strand of comparative analysis is “constant comparative analysis,” which stems from the grounded theory methodology of Barney Glaser and Anselm Strauss. It involves taking one entity or piece of data, such as a statement, an interview, or a theme, and comparing it with others to identify similarities or differences. By isolating these aspects, it is then possible to develop a conceptual model of the possible relations between various entities.

Researchers may, for example, compare the accounts or experiences of two different people who experienced the same event or are in similar contexts to engage in analytic accounts of why there are differences and how these two individuals’ experiences are related to one another. Comparative analysis is also a primary task within case study research. Case studies are often compiled with the knowledge that comparisons will be made with the description of a particular case. In some instances, researchers will compare a particular case with that of a hypothetical reference group or frame of reference to highlight differences (Analysis, 2022).

Semi Structured Interviews

The semi structured interview consisted of the interviewer, a scribe, and the interviewee. The same interviewer and scribe were present for all interviews. At the start of the interview, the interviewer described the need for the interview and how it fit into the overall risk assessment process. The first step in any risk assessment is problem formulation and the identification of information that is what questions is the cyber security risk assessment trying to answer and what information is available to answer those questions.

The semi structured interview consisted of questions about the tasks and management goals necessary to achieve progress in each interviewee's respective research area and the types of risks posed to each research area. Interviewees were also asked for their definitions of cyber security and cyber security risk. Each semi structured interview lasted approximately 30–60 minutes (Interviews, 2022).

Interviewing Authorities

The focus of this research is to derive the structure to improve the robustness of security policy of higher educational institutions, so the methodologies involved in this research is achieved through evaluating the standards of security policy of the higher educational institutions and to convey the ways to increase the security posture of their institutions through implementing the robust security policies.

This research involved in comparative analysis of security policies of two universities in United Kingdom which is based on adversary tactics, techniques and procedures involved and meeting the objectives of major international security standards and frameworks of cyber security in their security policy and essential steps involved in the security policy to meet the security standards the security policy of namely Buckinghamshire New University and University of Exeter also to semi structured interview with Mr Matt Hiely-Rayner who was the Director of Strategic Planning and Change at Buckinghamshire New University about to discuss about his view on cybersecurity in higher educational institutions, case studies of ransomware attacks in universities in united kingdom, need of data breach and incident response policies in the higher educational universities and role of robust security policy in making impact on business management of higher educational institutions and cyber threats also the techniques which universities are taking to mitigate those to maintain organisational resilience of the university and involved semi structured interview with Mrs Nirosha Holton who was the Senior Lecturer and Cyber Security Practitioner at University of Exeter about her sharing her view on cyber security impact on higher educational institution, need of robustness of security policy to any universities or organisations and tactics and techniques used to tackle the important cyber threats to higher educational institutions to business continuity of the institutions. The comparative analysis and measure of standards involved in it also the thoughts of two interviews and security policies of two institutions are considered as part of the research on assessing robustness of the security policy is measured also thereby defines the security posture and also point out areas in the security policy needs to be improved in two security policy which are taken part in the research to maintain the organisational resilience to tackle the cyber threats of the institutions.

Findings

Common Practices in Information Security Policies

Buckinghamshire New University and University of Exeter Policies

Acceptable Use Policy

Generally, it discusses how to utilise the internet and digital technology in a secure, acceptable, and responsible manner. It should be used as a template or tailored to meet the unique conditions and needs of each institution (ISP Exeter, 2022). It is a very significant document since the reason for having an Acceptable Use Policy (AUP) is to support effective practise and safe, ethical use of the internet and digital technology. Its key objectives are to raise awareness among students, parents, and teachers about the internet and modern devices potential as a beneficial learning resource also to determine the university's approach for encouraging secure Internet use and addressing the dangers connected with it and to offer protection under the law for universities from liabilities (ISP BNU, 2022).

Although describing why an AUP occurs and how it works may seem simple, it is nevertheless a crucial step in creating awareness and giving students with study of diverse digital technology and Information safety problems. While regulatory and technological solutions are critical, their usage should be tempered by teaching students to be accountable. Student education is a vital component of the university's virtual learning strategy (ISP Exeter, 2022).

Data Protection

Data protection policy should apply to all information kept by the institutions main architecture, including on-premises storage facilities, offsite facilities, and cloud storage. It should benefit the organization in strengthening the safety and integrity of all data, both at transit and at rest. Data security policies may indicate an institution's dedication to the security and privacy of customer information (ISP Exeter, 2022). If the business is subjected to compliance audits or suffers a data leak, the data security policy can be used to demonstrate the firm's adherence to data protection laws. A data security policy should include the provisions such as the extent to which data protection is essential to users, groups, technologies, and IT ecosystems are all using information security approaches and regulations. Any relevant data protection law or compliance requirements (ISP BNU, 2022).

Bring Your Own Device Policy (BYOD)

Information Security professionals and positions specifically liable for information security activities are examples of data security roles and responsibilities. The IT teams must decide whether and how to safeguard personal devices and set access levels.

Above all, a specified BYOD security policy should advise and enhance teaching and learning on how to use BYOD without jeopardising business data or networks (ISP Exeter, 2022). Categories of allowed devices are important components of BYOD policy. Policies governing data security and ownership Personal gadgets are given different levels of IT assistance. BYOD security should be linked with overall IT security and acceptable usage regulations. When IT administrators decide how much support to give to personal devices, they must strike a balance between corporate security and people' individual privacy (ISP BNU, 2022).

Email Security

The relevance of a strong Internet and email usage policy in a corporation is that it enables for efficient administration and management of the Internet in the business. These rules should outline proper Internet use for workers so that they aware of what is expected of them, as well as the surveillance and supervision need so that staff are informed of their rights to privacy. The regulations serve as a basis for any legal action taken against workers, and they also serve as a deterrent because staffs are informed that their internet and emails are indeed being tracked. A strong email policy must prioritize security (ISP Exeter, 2022).

Because email is the most common source of threats and cyber-attacks, businesses should spend in training company personnel (ISP Exeter, 2022). In business email policy, state clearly whatever the primary hazards are and how to recognize them, including such phishing and ransomware. Also, it's profitable to spend in email security training and software, such as anti-spam and Secure Email Gateway (ISP BNU, 2022).

Password policy

A password policy is a collection of guidelines designed to improve computer security by encouraging users to develop reliable, secure passwords and then properly store and use them. A password policy is often part of an institution's formal policies and may be used as part of security awareness campaign (ISP Exeter, 2022). Passwords are your first line of defence against illegal access to the device. The harder the pass code, the more secure your system will be against dangerous software and attackers. A secure password is more than just one password; it is critical that you ensure secure passwords for every account that you connect via your machine. When using a business network, the security team may advise you to utilize secure and strong password policy (ISP BNU, 2022).

Malware policy

The incidence of information security events including malware attacks, as well as the cost of potential disruption and service restoration, continues to rise. Deploying anti malware and antivirus technologies, barring unauthorized network and access to a computer, increasing user security awareness, and rapid recognition and remediation of data breaches are all best practices that must be followed to mitigate activities and mitigate the computing environment.

To preserve the integrity, availability, and efficiency of University IT infrastructure, the University periodically reviews traffic on the network infrastructure and devices linked to the network system, including activities and traffic originating off university (ISP Exeter, 2022). This comprises (but is not limited to) surveillance for infected computers and other viruses, compliance issues, performance of computing devices, unauthorized access to systems of institutions of higher learning, and so on (ISP BNU, 2022).

Uniqueness in Information Security Policies:

University of Exeter Policy

Incident and Response Team

There is an old saying in information security of "it's not if, but when". Whether it's a targeted attack, stealing data and resources, or a breach of policy by a network administrator, at some point your organisation is going to be faced with a cyber-related incident.

In today's climate having access to the right skills at the right time is essential to managing the risks posed by a cyber-attack. More often, the damage is caused by a failed response to an incident, not the point of the attack. An inadequate response could quickly turn an incident into a crisis (ISP Exeter, 2022).

IT security Team

The Information Security Team strives to be a high visibility, proactive, and successful team that supports the department and the larger collegiate-University to achieve its strategic goals by lowering the potential for serious security events and security breaches (ISP BNU, 2022). Because of the growing quantity and effectiveness of cyber-attacks, data theft, and cyber forgery, we require effective and strong security throughout the entire University.

The Information Security Team (IST) offers aid and direction to ensure that our teaching, management, research, and cooperation are as safe as feasible. Our objectives are to promote educated and protection decisions to enable safe research, cooperation, education, and management. Control and evaluate technical risks to Academic systems and data (ISP Exeter, 2022). Manage the design and deployment of highly safe information technology systems across the institutions.

Exchange ideas and cultivate a comprehensive security culture throughout the Institution. The IST specializes in providing help and resources to units, departments, and professionals so that they may adopt appropriate security measures and manage those risks efficiently. The IST needs to provide range of services to assist in achieving these objectives (ISP Exeter, 2022).

Data breach Policy

This Data Breach Policy outlines the measures that should be performed in the event of a security incident. This documentation has been revised to comply with the GDPR in the United Kingdom. It will be operational in early 2021. A data breach (which may or may not contain personally identifiable information) can take numerous forms (ISP Exeter, 2022).

It might entail data loss or theft, illegal access to, utilization, or alteration of data, or maybe something seemingly less obvious like equipment failures, human mistake, or equipment loss or theft. Data breaches, whether alleged or genuine, should be submitted to the relevant person (or division) within organization. That may be Data Protection Officer or authorized person responsible for data security in each university and it is very critical to precisely identify this line of communication (ISP Exeter, 2022).

Buckinghamshire New University Policy

Social Media Policy

A specification of social media policy is a set that describes how a company, and its workers should behave digitally. It gives advice and instructions on how to protect the business reputation on media platforms and educates staff on ethics and professional behavioural knowledge. The strategic plan for social media is often a multi-page documentation that is stored on a university intranet. It will comprise the things to avoid and things to follow, regulatory or compliance duties, and standards for digital behaviours of faculties (ISP BNU, 2022).

As part of the agreement framework between staffs, many institutions will give the social media policy now of new employee orientation. It will also be discussed throughout the new staff induction process (ISP BNU, 2022).

Freedom of Information Policy

The Freedom of Information (FOI) Act, enacted in 2000, replaced the Open Government Code of Practice, which had been in effect since 1994. The Provision gives the wider populace general access to practically all forms of recorded data kept by governmental entities. The Regulation of this act went full force on January 1, 2005.

This act requires public entities to disclose details of any documentation that they possess and to provide the general populace access to the data on request, unless an exception exists, such as private or other confidential communications (ISP BNU, 2022). The Freedom of Information Act is fully retroactive and applies to any information kept by public agencies independently of its time. It's doesn't require public agencies to keep data that is no longer applicable to them. The Information Commissioner oversees monitoring organization compliance, issuing assurances, serving data and investigative notifications, and, if necessary, initiating judicial procedures to guarantee compliance. According to certain restrictions and limitations, this act grants the public a fundamental right to access information kept by public entities. There are no restrictions on who can seek access to sensitive content or for what reason. Whenever feasible and within the scope, the institutions are dedicated to the concepts of public access to reliable information and data according to the principles drawn in the act under its framework (ISP BNU, 2022).

Results

Buckinghamshire New University

In the security policy of the Buckinghamshire New University freedom of information and social media policy is the latest addition to the security policy which satisfies the need in reviewing the security in an appropriate timeline to counter the latest cyber threats to the organisations in an excellent manner but in the brief in the social media policy is not presented well there is lack of social media platforms that the students are permitted to use in the campus because there are thousands of vulnerable social media platforms are outside in internet and some not appropriate to the students which could be act a way to penetrate the university internal network (ISP BNU, 2022). In freedom of information policy, the type of information which is should allowed to express such some information may harm some audiences and fake information propaganda against others which may harm their reputation and the consequences negative utilization of freedom of information is not briefed in the security policy so the critical thinking usage of assets and permissions allowed which impact on both positive and negative sides so the safe guarding the rights and reputation of students, faculties and employees is primary functions of any higher educational institutions (ISP BNU, 2022). In security awareness training policy, some appropriate responsibility which is mentioned in the policy is drafted with ‘should’ not with the ‘must’ meaning the responsibilities is may be followed not a mandatory thing to follows which leads to the weakness in the security policy because every employee needs to get appropriate security awareness training that is the mandatory thing and security policy is reviewed last in June 2016 and that is not up to robust security mark reviewing and assessing the security assets is very crucial at least once in every year which help the organisations to obtain the better knowledge about their cyber assets. In the process of risk assessment section of the security policy the techniques and ways to assess the resources (ISP BNU, 2022). The most advance techniques of risk assessment are done through penetration testing (Red Teaming) is not placed in the part of security policy which is highly recommended according to the current threat landscape. The Information Technology (IT) Security Team and Chief Information Security Officer is most crucial thing for an organisation which is dealing security as their main concern. Most of the universities think that IT security is the part of IT, but the main responsibility of IT Team is to maintain the functionality of the organisation and the main responsibility of IT security team to maintain the security of the organisation so the lack of positioning the IT security is weakness of an organisation. Incident response team is not included in the part of policy which is more important for every organisation to take necessary steps which is responsible every organisation for their business continuity after it is affected by any disaster like data theft and retain their business position which plays a significant part of the security policy and the assets management should be defined in brief manner and how the resources or the techniques where the resources are reviewed should be defined in the policy (ISP BNU, 2022).

University of Exeter

In the security policy of University of Exeter has an IT security Team is positive side of an organisation but the security policy is last reviewed in September 2019 that is not up to robust security mark reviewing and assessing the security assets is very crucial at least once in every year which help the organisations to obtain the better knowledge about their cyber assets. The latest trends of security policy like social media policy and freedom of information are not included on the security policy because it is mandatory to follow latest trends and added those necessary security measures to the security policy makes the policy more robust to defend against the security threats to an organisation In Malware policy of the security policy there is all latest malware threats are not updated which is very crucial to update malware policy because in today's threats landscape malwares are largest and its evolved very frequently. There is the need of updating the malware policy is very important for every organisation which consider security as their major concern to protect their cyber assets effectively. The ISO Standards are not mentioned in the security policy which is mandatory to follow the international security standards which is mandatory for every organisation to construct their security policy which able to assess their own security policy is up to the mark and provide enough elements which is to be considered when constructing the security policy which is more robust to defend against the cyber threats and safeguard the confidentiality, integrity and availability of the organisations. The security assessment and the techniques involved in it is not properly briefed and techniques involved in the risk assessment are not discussed in the security policy (ISP Exeter, 2022).

Discussion

Interview on authorities:

Buckinghamshire New University:

Interview with Mr Matt Hiely-Rayner

Designation: Director of Strategic Planning and Change

The discussion on security measures in Buckinghamshire New University and the importance of security policy impacts on higher educational institutions with Mr Matt Hiely-Rayner is held on 31 May 2022. On discussing about security concerns about the university management Matt said that university get more involved about security threats on higher educational institutional organisation after few institutions in United Kingdom get affected by ransomware attacks. On discussion about risk assessment and techniques involved in its matt said that risk assessment of resources is done by IT Team and conveyed that there is no IT Security Team in the university also said university management is considering on constructing security team and techniques followed on risk assessment is very basic and outdated techniques used to assess the resources.

Matt said that IT Team is built a proposal for adding funds from the university management to upgrade the security management of the university. Matt agreed that security measures is not up to the mark when briefly discussed about the about risk assessments techniques like penetration testing. On discussion about the Matt said about security awareness is provided by IT team such as phishing emails are sent to employees to examine the security awareness the organisations. On discussion about security upgrade of the resources of the university matt said that university focusing on upgrade of security of the resources is on purchasing high end equipment's will improve the security features of the resources and matt agreed management focusing on purchasing high end equipment's rather than implementing the security techniques to robust the security management of the university (ISP BNU, 2022).

University of Exeter

Interview with Mrs Nirosha Holton

Designation: Senior Lecturer on Organisational Resilience

The discussion on security measures in University of Exeter and the importance of security policy impacts on higher educational institutions with Mrs Nirosha Holton is held on 6 June 2022. On discussing about the security concern about management of the university Nirosha said that the university had form IT security team after the university is attacked by the ransomware attack and there is no proper backup procedures are followed by the university when the university hit by ransomware so the university had not pay the ransom but in other hand it loses many information of the international students and employee details which is stored in their database and this due there is no incident response team and business continuity policy is not been drafted.

On the discussion of the outdated malware policy and the outdated reviewed of the security policy of the university since September 2019, Nirosha said that IT security team is on organising the team to update the malware and audit the security resources of the university is under proposal on receiving the funds from the university to upgrade the security posture of the university. Nirosha also added that IT security team of university comparatively very small to the IT Team of the university.

On discussion about the modern techniques to be enrolled in the data breach policy Nirosha said that concept of vulnerability disclosure program is on the stage to be added in the policy within the few months it will provide the students to report the vulnerability of the university which help the university help to counter the zero-day vulnerability which is biggest threat to higher educational institutions (ISP Exeter, 2022).

Conclusions

This study aimed at a better understanding of the impact of key organizational groups perceptions of information security policies (ISPs) on information security policy implementation and use in an organizational context. To this end, research have extended the existing literature on frames of reference and information security policies by proposing the several main concept of viewpoints of reference in Information Security Policy and by suggesting that it provides a means for analysing employees perceptions of ISP. We have further posited that ISP congruence and incongruence among organizational groups afford an understanding of the consequences of those perceptions to organization's information security management. The study was conducted as an interpretive case study and was guided by two research questions and a theoretical framework that builds on and extends the literature on frames of reference and on ISPs. Regarding the first research question of the study which comprises how do different organizational groups perceive organization's information security policies? Also briefs future work beyond answering the objectives of the questions.

This study illustrates that organizational groups' perceptions of ISPs do not only reflect the intrinsic qualities of the ISP documents. Indeed, to understand how different organizational groups perceive the organizational ISPs, we must understand the group's role regarding the ISPs, the interaction the group has with the ISPs and the context in which ISPs are embedded in. Therefore, emphasizing the structure or content of the ISP documents is not sufficient but needs to be augmented with an understanding of organizational groups expectations and interpretations of Is. Concerning the study's second research questions are what are the consequences of organizational groups' perceptions of information security policies? in this study, viewpoints of reference in information security policy incongruence among organizational groups appeared as frustration, resistance, false assumptions, and conflicting expectations of the ISPs, their implementation and use. It furthermore, accounted for some of the decisions leading to ineffective information security management practices. Consequently, the incongruence in organizational groups viewpoints of reference in reference in information security policy provides one explanation for adversities and unanticipated outcomes around ISP implementation and use in an organizational context.

Recommendations and Future Work

The recommendation of this research is suggested by supervisor to conduct deeper interpretation and comparative analysis of more Information Security Policy of several higher educational institutions will provide the holistic view security concerns which is being implemented in the higher educational institution Research often uncovers more questions than what it answered.

Indeed, as our understanding evolved, many new questions came to our minds. The positive aspect is that it gives new ideas for further research. The future work of this work will address some of these new routes for future research that involves being worthwhile to address and that are the most closely related to the topic of this study. This is to say that many of the questions that rose during the study were quite widely related to the field of information security management.

Firstly, research on information security policies should take a closer look into the ways different groups expectations can be brought closer to each other. This could be achieved, for example, by studying how the different organizational groups viewpoints of reference in information security policy could approach congruence.

Secondly, the frames do not only change in content, but also in structure and provide clear suggestion to involve in more research in exploring more techniques and tactics which is involved in risk assessments and taking steps to conduct interviews the respective administrative authorities in several universities to discuss how to implement those techniques in the universities thereby the goal of the research to build a robust security posture of higher educational institutions.

References

Alassaf, M. and Alkhalifah, A. (2021) 'Exploring the Influence of Direct and Indirect Factors on Information Security Policy Compliance: A Systematic Literature Review', IEEE Access, 9, pp. 162687-162705.

AMT (2022) Academic integrity and misconduct - The University of Nottingham. Available at: https://www.nottingham.ac.uk/studyingeffectively/studying/integrity/index.aspx (Accessed: 2 June 2022).

Analysis (2022) How to Write a Comparative Analysis. Available at: https://writingcenter.fas.harvard.edu/pages/how-write-comparative-analysis (Accessed: 9 June 2022).

Arkansas (2022) Threats to Academic Integrity. University of Arkansas Global Campus. Available at: https://globalcampus.uark.edu/instructional-design/new-to-online-teaching/03-threats-academic-integrity.php (Accessed: 2 June 2022).

Azeus (2022) Best practices in business continuity planning for higher education. Available at: https://www.azeusconvene.com/articles/best-practices-in-business-continuity-planning-for-higher-education (Accessed: 2 June 2022).

Backups (2022) What Is Backup and Recovery? - Why It's Important | NetApp. Available at: https://www.netapp.com/data-protection/backup-recovery/what-is-backup-recovery/ (Accessed: 1 June 2022).

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).

Bio Melbourne Network (2022) Importance of acceptable use policy – IT Systems & Services | Bio Melbourne Network. Available at: https://biomelbourne.org/importance-of-acceptable-use-policy-it-systems-services/ (Accessed: 31 May 2022).

Blog, S. (2022) Overcoming challenges of remote learning with educational technology. Available at: https://blog.sanako.com/overcoming-challenges-of-remote-learning (Accessed: 2 June 2022).

Business Continuity (2022) Information Security Aspects of Business Continuity Management Standard - Winston-Salem State University. Available at: https://www.wssu.edu/about/offices-and-departments/the-office-of-information-technology/it-security-standards/information-security-aspects-of-business-continuity-management-standard.html (Accessed: 2 June 2022).

CHAS (2022a) Why Are Risk Assessments Important? | CHAS. Available at: https://www.chas.co.uk/help-advice/risk-management-compliance/risk-assessment-introduction/risk-assessment-importance/ (Accessed: 1 June 2022).

CHAS (2022b) What Are the Types of Risk Assessments? | CHAS. Available at: https://www.chas.co.uk/help-advice/risk-management-compliance/risk-safety-statement-types/ (Accessed: 8 June 2022).

Cisco, P. (2022) What Is Information Security (InfoSec)? Available at: https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html (Accessed: 31 May 2022).

CISO (2022) Nearly half of firms still don't have a CISO. Available at: https://www.techradar.com/uk/news/nearly-half-of-firms-still-dont-have-a-ciso (Accessed: 1 June 2022).

Duigan, A.N. (2022) 10 steps to a successful security policy. Available at: https://www.computerworld.com/article/2572970/10-steps-to-a-successful-security-policy.html (Accessed: 31 May 2022).

Enterprisersproject.com (2022) How to create an effective security policy: 6 tips. Available at: https://enterprisersproject.com/article/2021/10/security-policy-how-to-create (Accessed: 31 May 2022).

F5 Networks (2022) What Is the CIA Triad? Available at: https://www.f5.com/labs/articles/education/what-is-the-cia-triad (Accessed: 31 May 2022).

FSB, T. (2022) Eight benefits of a cyber security policy. Available at: https://www.fsb.org.uk/resources-page/8-benefits-of-a-cyber-security-policy.html (Accessed: 31 May 2022).

IBM.com (2022) IBM Docs. Available at: https://www.ibm.com/docs/en/i/7.4?topic=strategy-developing-security-policy (Accessed: 31 May 2022).

ICO (2022) The principles. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ (Accessed: 2 June 2022).

Interviews (2022) What Is a Semi-Structured Interview? Available at: https://www.thebalancecareers.com/what-is-a-semi-structured-interview-2061632 (Accessed: 9 June 2022).

Irwin, L. (2022) Guide to ISO 27001 Physical and Environmental Security. Available at: https://www.vigilantsoftware.co.uk/blog/guide-to-iso-27001-physical-and-environmental-security (Accessed: 31 May 2022).

ISP BNU (2022) Information Security Policy. Available at: https://www.bucks.ac.uk/sites/default/files/2021-04/Information%20Security%20Policy.pdf (Accessed: 9 June 2022).

ISP Exeter (2022) Information Security Controls Policy. Available at: http://www.exeter.ac.uk/media/level1/academicserviceswebsite/it/recordsmanagementservice/policydocuments/Information_Security_Controls_Policy_v2.pdf (Accessed: 9 June 2022).

ISO Governance (2022) ISO 27001. Available at: https://www.itgovernance.co.uk/iso27001 (Accessed: 31 May 2022).

IT Asset (2022) What is IT asset management? A guide | Atlassian. Available at: https://www.atlassian.com/itsm/it-asset-management (Accessed: 2 June 2022).

Macnish, K. and van der Ham, J. (2020) 'Ethics in cybersecurity research and practice', Technology in Society, 63, p. 101382.

NCSC (2022) Alert: Targeted ransomware attacks on UK education sector. Available at: https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector (Accessed: 1 June 2022).

Nibusinessinfo.co.uk (2022) Different types of IT risk | nibusinessinfo.co.uk. Available at: https://www.nibusinessinfo.co.uk/content/different-types-it-risk (Accessed: 8 June 2022).

NIST, N. (2022) Information Security Policies According to NIST - Information Shield. Available at: https://informationshield.com/2013/05/08/information-security-policies-according-to-nist/ (Accessed: 31 May 2022).

Norton (2022) What is encryption and how does it protect your data? Available at: https://us.norton.com/internetsecurity-privacy-what-is-encryption.html (Accessed: 1 June 2022).

OAuth (2022) Authentication vs. Authorization. Available at: https://auth0.com/docs/get-started/identity-fundamentals/authentication-and-authorization (Accessed: 31 May 2022).

OWASP (2022) SQL Injection | OWASP Foundation. Available at: https://owasp.org/www-community/attacks/SQL_Injection (Accessed: 1 June 2022).

Palo Alto Networks (2022) What is an IT Security Policy? Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-an-it-security-policy (Accessed: 31 May 2022).

Phishing (2022) What is phishing | Attack techniques & scam examples | Imperva. Available at: https://www.imperva.com/learn/application-security/phishing-attack-scam/ (Accessed: 2 June 2022).

Plesk (2022) Backup Importance, Its Types and Strategies. Available at: https://www.plesk.com/blog/various/backup-importance-its-types-and-strategies/ (Accessed: 1 June 2022).

Ransomware (2022) What is Ransomware? | How to Protect Against Ransomware. Available at: https://www.malwarebytes.com/ransomware (Accessed: 1 June 2022).

Rapid 7 (2022) Defining the Roles & Responsibilities of Your Security Team | Rapid7 Blog. Available at: https://www.rapid7.com/blog/post/2016/08/18/defining-the-roles-responsibilities-of-your-security-team/ (Accessed: 2 June 2022).

Sailpoint (2022) Identity for Access Management. Available at: https://www.sailpoint.com/integrations/access-management/ (Accessed: 31 May 2022).

Sail point (2022) Identity for Access Management. Available at: https://www.sailpoint.com/integrations/access-management/ (Accessed: 31 May 2022).

Sans.org (2022) ISP Templates | SANS Institute. Available at: https://www.sans.org/information-security-policy/ (Accessed: 31 May 2022).

Search data, D. (2022) What is Data Protection and Why is it Important? Definition from WhatIs.com. Available at: https://www.techtarget.com/searchdatabackup/definition/data-protection (Accessed: 2 June 2022).

Smith, D. (2022) 38875.pdf on Egnyte. Available at: https://sansorg.egnyte.com/dl/ibhUAbTFr7 (Accessed: 31 May 2022).

SQLi (2022) What is SQL Injection | SQLI Attack Example & Prevention Methods | Imperva. Available at: https://www.imperva.com/learn/application-security/sql-injection-sqli/ (Accessed: 1 June 2022).

Stack (2022) Cybersecurity On EU. Available at: https://thestack.technology/nis-2-nis-directive-replacement/ (Accessed: 8 June 2022).

Tang, C. and Xie, Y. (2010) 'Description and Reasoning of Security Policy in Information System Based on Security Domain', 2010 2nd International Symposium on Information Engineering and Electronic Commerce.

Toptal (2022) Cybersecurity in Higher Education: Problems and Solutions. Available at: https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education (Accessed: 1 June 2022).

UK Universities (2022) Latest blog - Colleges and Universities in the UK targeted by cyber-attacks during the pandemic - Tech force. Available at: https://techforce.co.uk/blog/2021/colleges-and-universities-in-the-uk-targeted-by-cyber-attacks-during-the-pandemic (Accessed: 1 June 2022).

Varonis.com (2022) How to Create a Good Security Policy. Available at: https://www.varonis.com/blog/how-to-create-a-good-security-policy (Accessed: 31 May 2022).

Appendices

Resilient Guidelines for Security Policy Implementation in Higher Educational Institution

Introduction

The Institution's operations are supported by information systems, which are critical to its educational, scientific, and administrative positions. It is consequently critical that all academic representatives contribute to ensuring the availability, integrity, confidentiality, and authenticity of the information they retain or receive. Mishandling of institutional material not only can ruin the university's brand and impair its operations, but it may also expose the institution to legal consequences. Furthermore, the lost or unintended revelation of personal information can generate great pain to those whose data is compromised. This report contains the institutions' Information Security Policy, as well as student and faculty guidelines. All University employees must follow the policies outlined in this document.

Scope and Purpose

This Policy offers a structure for managing information security across the Institution and pertains to:

- Professionals, Lecturers, students, outsiders, and private vendors who have access to academic information systems.
- All data or information is kept by the Institution in print or electronic media, including papers, reports, and other printed and digital data, photographs, and multimedia.

- All systems are connected to the institution's digital or telephone networks, as well as any technologies provided by the institution.
- All information generated by the Institution during its administrative operations, whether handled digitally or on hardcopy, including all interactions transmitted to or from the Institution and any Academic information kept on platforms outside the Campus's network.

- All Institute-owned and personalized portable computing devices, as well as Institute non-mobile personal computers, are utilized to access the Institution's Information Systems. Non-mobile devices, including individually owned desktops and laptops used to access Academic material outside of the university campus, are also covered by this Regulation.
- All independent third-party partners who provide operations to the Institution in the areas of data processing and decision-making activities.

Definitions

The following defined attributes are applicable for the purposes of this report:

Computer - Covers all end-user computing devices and networking devices, even if they're not located on institution premises.

Data - According to the Data Protection Act, information is collected that includes

- Is processed using technology that operates continuously in response to instructions supplied for that objective.
- Is collected with the aim of being analyzed using such technology,
- Is documented as part of a relevant file system or with the goal of becoming part of significant file management,

Encryption - Encryption is a mathematical representation that encodes data using a secret key such that only those users who have access to the key may decode and access the information. In many circumstances, encryption can offer sufficient protection against unauthorized or illegal transfer of personal information, particularly when alternate safeguards cannot be implemented (ISP BNU, 2022).

Information – For the purposes of this reporting policy, the terms 'information' and 'data' are comparable

Mobile Computing Device - A mobile communication device is any portable computational or networking device that can process data. Laptop computers, tablets, and smartphones are among examples.

Personal Data - Personal data refers to data/information relating to a live, identifiable individual. i.e., based on the data, or from the data and other information in the data controller's custody or tend to come into knowledge, and any statement of opinion on the individual, as well as any evidence of the information controller's or any other group's interests towards the individual entity.

Mobile Devices: A mobile computing device is defined as any transportable computing or mobile networking device that may be utilized to communicate information. External hard discs or solid-state disks, Flash drives, and memory cards are all examples.

Sensitive Personal Data: All information on an individual's personal racial or ethnic origin, political ideas, religious beliefs, labor union activity, provision of health care, sexual life, or details of criminal offenses.

Software management: It refers to any technology acquisition, development, deployment, licensing, administration, or deletion that occurs on computers leased, controlled, or used by the institution.

Governance

The Head of Information Assurance is responsible for the creation, management, and dissemination of this Information Security Policy. The Vice Chancellor's Advisory Group (VCAG) has authorized this Information Security Policy, and any significant modifications must be implemented with the agreement of VCAG. This Information Security Policy will be reviewed on a regular basis, and VCAG will be responsible for ensuring that these assessments take place. It is also VCAG's obligation to ensure that the Policy is and stays logical and consistent.

Information Security Principles

The University recognizes that data is a crucial necessity for an awareness-driven institution, and it is the Institution's policy to safeguard the data it manages from the negative consequences of breakdowns in confidentiality, integrity, availability, and legislative compliance that might occur alternatively. The achievement of this goal is contingent on all academic staff and students adhering to this policy.

The Eight Principles of Information Security

To underlie its Information Security Policy, the Institution has established the eight principles listed below:

- Information shall be safeguarded in accordance with all applicable academic rules and regulations, including those associated with information protection, right to information, and individual rights.
- Every information which may be an intangible asset will have a designated owner who are responsible for identifying approved information usage and guaranteeing that suitable safeguards are in place to secure the information infrastructure.
- Only those with a valid in need of accessibility will be granted access to information.
- Data shall be categorized in accordance with the Institution's data classification rules.

- Data integrity shall be protected.
- All persons who have been provided accessibility must treat it responsibly in line with its categorization.
- Data shall be safeguarded against illegal access.
- Any action that violates the rules of the Information Security Policy and its related policies shall be handled through the Student or Staff Disciplinary Procedures.

Policy Principles

The following protocols and procedures must be followed to guarantee that a new information system is created with user privacy precautions in mind from the start. These criteria define the elevated policies and protocols that must be implemented when designing new Academic information systems (ISP BNU, 2022).

Security Concern Steps

Secure Configurations

Critical security control is developing and proactively preserving the secure configuration of systems. Vulnerabilities must be addressed, which is normally accomplished by frequent patching. Technologies that are not the management of the employees are exposed to threats that may have been avoided (ISP Exeter, 2022).

Network Security

Networks must be safeguarded against both internal and external attacks. This is often accomplished by an authoritative structure with academic standards established and implementing suitable organizational and technological controls. Failure to adequately defend academic networks leaves the institution open to a range of threats (ISP Exeter, 2022).

Managing user privileges

The University must determine what degree of exposure workers require to data, products, services, and assets to execute their tasks; otherwise, those in charge will be unable to control user granular permissions efficiently. All users must be granted a fair (but basic) set of system privileges and permissions according to their function. The delegation of very elevated system rights must be properly monitored and maintained. Failing to manage rights properly increases the danger of power abuse, enhanced attack capacity, and the potential to circumvent current security safeguards (ISP BNU, 2022).

User education and awareness

All All-Academic representatives have a vital role in supporting to safeguarding the organization, and that shouldn't impair their capacity to do so. All employees must take the necessary Information Governance training. Customized training, advice, and consistency with the requirements should be in operation for every system-specific technology. Those having enhanced system rights must get additional training and/or mentoring.

Inability to properly assist users with the necessary tools and understanding may expose the Institution to risks such as legal regulatory penalties, lack of reporting of disclosure incidents of security events, and major offensive.

Incident response and management

Security events will certainly occur, and their severity may differ. All events must be managed and controlled, especially those that are significant enough to necessitate the use of business continuity or disaster recovery plans (ISP Exeter, 2022).

In many HEIs, security policies are documented but not continuously monitored for compliance. By integrating Security Information and Event Management (SIEM) tools (such as Splunk or Microsoft Sentinel) and Security Orchestration, Automation, and Response (SOAR) platforms, institutions can translate static policy documents into dynamic, enforceable controls.

For example, a security policy that limits failed login attempts can be technically enforced using a SIEM rule that detects brute-force activity, while a SOAR playbook can lock the account and notify the administrator in real time. Similarly, email policies can be enforced through automated phishing detection rules that quarantine messages without manual intervention. These integrations ensure that policies are not only defined but are executed continuously and consistently through automated workflows. In accordance with implementing policies, the institution will enhance its disaster response capabilities to identify, handle, and evaluate security risks.

Malware prevention

Malware (malicious software) can cause severe damage to digital infrastructures, such as the interruption of vital business systems and the unlawful transmission of confidential information or data destruction. The tools used to implant malware encompass the whole network infrastructure, increasing the danger of intrusion. The Anti-Malware policy and installing suitable anti-malware measures inside each technology as part of a comprehensive 'defense in depth' approach can help to geek about knowledge of the threat factors (ISP BNU, 2022).

Monitoring

Supervision and Surveillance allows you to examine how devices are utilized and if they really are being hacked. The administration may not even be able to notice or respond to assaults, or report for activities if we do not have the responsibility to control campus network infrastructure (ISP Exeter, 2022).

Adopting Zero Trust in Educational Environments

A Zero Trust security model, where no device or user is inherently trusted—even within the network perimeter—offers a more robust alternative to traditional perimeter-based models. Implementation involves enforcing least privilege access, multi-factor authentication (MFA), identity-based segmentation, and continuous risk assessment. HEIs can reflect these principles in policy by defining access tiers for staff, faculty, and students, and by controlling resource access through role-based access controls (RBAC) and identity federation tools.

Removable media

Detachable media allows for the transmission and storage of large amounts of sensitive data, or the importation of offensive content. Failing to follow any safeguards on external storage might expose the institution to the consequences of loss of data, virus insertion, and reputational harm (ISP BNU, 2022).

Staff should exercise extra caution while using personal devices, which poses a larger risk than material stored on institutional networks (ISP BNU, 2022).

Mobile and remote working

Mobile working and remote access enhance information transit and storage (or management of the network) beyond the institution's infrastructure, generally over the external network. Mobile devices are also often utilized in places where there is a danger of display monitoring or device breaches. As a result, the institutions must develop robust mobile working protocols and procedures to reduce these risks. Supervisors or Security teams must guarantee that the security policy is followed (ISP Exeter, 2022).

Personally enabled devices

The Institution understands the need for adaptable working methods in a multicultural workplace. Improper planning of unsecured devices, on the other hand, potentially results in unwanted access to important personal or organizational information, as well as compromising core resources or important infrastructure (ISP BNU, 2022).

Conclusion

This Information Security Policy framework is designed to provide a structured, enforceable, and adaptable approach to protecting the confidentiality, integrity, availability, and lawful use of academic and administrative information within Higher Educational Institutions. By outlining core security principles, governance responsibilities, and specific procedural guidelines including incident response, asset control, user access management, mobile computing, and Zero Trust implementation—this policy equips institutions with the tools to address emerging cybersecurity risks in an increasingly digital and decentralized learning environment.

All stakeholders including academic staff, students, third-party vendors, and technical administrators share a collective responsibility to uphold this policy through continuous vigilance, compliance, and proactive reporting. The policy will be subject to regular review and updates to reflect advancements in technology, regulatory changes, and institutional requirements, ensuring that security remains an embedded, evolving, and resilient function of the academic and research community.