Assignment 2

Vedant Marwadi - NXJ4679 [1]

[1]Master of Computer and Information Science , Cybercrime and Cybersecurity, Auckland University of Technology

1. PART 1

The COVID-19 widespread triggered critical changes in the Information and Communication Technologies (ICT) approaches due to the challenges and openings exposed by the emergency. The introductory reaction to the pandemic shifted broadly across nations, and ICT policies have never been the same ever since. ICT stages initially planned for other purposes were repurposed to meet commerce needs amid the widespread (Yang et al., 2020).

It could be seen that the lockdown constrained numerous companies to extend their proximity and shift towards remote work. Within the EU, for instance, 33% of enterprises expanded the share of staff having remote access to company's email or other ICT frameworks, and 91% of these firms did so more or less due to COVID-19 ('Impact of COVID-19 on the use of ICT in enterprises', 2022). In addition, organizations developed and implemented working environment policies to support ICT-supported remote working (Davies, 2021). Moreover, multiple businesses have invested in digital technologies such as computers and laptops. These investments have been significant in empowering workers to work remotely, maintain communication, and coordinate with their co-workers ('The pandemic has boosted firm investments in digital technologies', 2021). Furthermore, nations took up Bring Your Own Device approaches to promote maintainability and reduce costs. The pandemic also steered a surge in distance learning in schools around the world as schools and colleges closed due to lockdowns. This move highlighted the requirement for digital infrastructure and assets in the education sector as well.

On the other side, in order to protect data and moderate potential dangers related to remote and hybrid work setups, ICT policies started to address data privacy and security concerns. On July 26, 2023, the Securities and Exchange Commission issued a new code to make sure companies are clearer about and responsible for managing cybersecurity risks ('SEC Issues New Requirements for Cybersecurity Disclosures', 2023). During the

second quarter of 2023, an unvarying trend could be seen from officials and regulators in tending to the dangers posed by AI. In addition to that, various legislative proposals have been presented, such as the National AI Commission Act and the AI Disclosure Act, which are centered on regulating AI tools and systems (Ponder, 2023). In December 2023, Dubai International Financial Centre framed a new rule to fix its data protection rules. It was made up to confirm that personal information of people is taken care of and is kept safe as well as private in the finance industry ('Data Privacy Day 2024 – Key Global Developments in Data Privacy and Cybersecurity in 2023 and What to Expect in 2024', 2024). In addition to that, to show how important it is to keep healthcare information safe, policymakers want small and medium-sized healthcare businesses to better manage digital security risks. This is especially important now that more healthcare tasks are being done online ('Seven lessons learned about digital security during the COVID-19 crisis', 2020). In October 2023, the FAR Council announced two new codes for cybersecurity that government contractors need to follow. These rules were for enterprises that work with the government (Damalouji, 2023).

From 2019 to 2023, there were huge changes in ICT policies, and looking ahead, it can be said that these trends are likely to continue in the future. The convenience and efficiency of remote work and online collaborations are without any doubt here to stay, which makes the ongoing investment in ICT infrastructure and security measures essential. The future of ICT will unquestionably be shaped by the lessons learned and adaptations made during this unprecedented global crisis.

2. PART 2

2.1 Introduction

The Computer Science Association of New Zealand (CSANZ) is a non-governmental organization (NGO) that speaks for and hypes computer science (CS) in New Zealand. CSANZ is also known for putting together activities in CS research as well as in teaching across numerous departments.

The Computer Science Association of New Zealand (CSANZ) is committed to the secure and responsible use of Information and Communication Technology (ICT) resources. This policy sketches and consolidates the expectations as well as requirements for all staff, employees, and visitors who utilize CSANZ ICT resources.

2.2 Policy Objectives

This policy aspires to accomplish the following objectives:

2.2.1 Information Security:

Protect the privacy, honesty, and availability of CSANZ information property.

2.2.2 Member Safety:

Ensure a safe and secure work environment for members and collaborators.

2.2.3 Beneficiaries and Stakeholder Protection:

Protect the privacy and security of beneficiaries and stakeholder information.

2.2.4 Compliance:

Ensure adherence to relevant laws and regulations regarding ICT use.

2.3 ICT Policy Attributes

2.3.1 Accountability and Responsibility

- CSANZ members and collaborators are liable for safeguarding their access to ICT resources by creating and maintaining strong, unique passwords for all accounts. Sharing passwords is strictly verboten. [Digital Identity Guidelines, NIST Special Publication (SP) 800-63B]
- CSANZ members and collaborators are entrusted with the physical security of their assigned ICT equipment, including laptops and mobile devices. This means taking pertinent and apropos prudence to protect these devices at all times. [Security and Privacy Controls for Federal Information Systems and Organizations (FISMA), NIST Special Publication (SP) 800-53, Revision 5]
- CSANZ members and collaborators play a cardinal character in protecting our organization from cyber threats. This encompasses diagnosing and informing believed spam and phishing attempts to the ICT department. [Phishing and Other Techniques for Attempting to Steal User Credentials and Data, NIST Special Publication (SP) 800-61, Revision 2]
- CSANZ members and collaborators are also obligated to at once report any suspected security incidents to the ICT department. This includes, but is not limited to, potential data breaches or malware infections. [Computer Security Incident Handling Guide, NIST Special Publication (SP) 800-61, Revision 2]

2.3.2 Acceptable Use

- ICT resources are accommodated by CSANZ for work-related functions solitary. Personal use is entitled on a limited basis, provided it does not interfere with work

duties, violate this policy, or consume excessive resources. [Security and Privacy Controls for Federal Information Systems and Organizations (FISMA), NIST Special Publication (SP) 800-53, Revision 5]

- CSANZ debar the downloading or distribution of illicit content, engaging in unauthorized online activities, and using the network for any malicious purpose. [Computer Fraud and Abuse Act (CFAA) 18 U.S.C. § 1030, 1986]

- CSANZ take advantage of social media for efficacious communication and engagement. However, to certify the uniformity and brand alignment, individuals must obtain prior authorization before representing CSANZ on their personal social media accounts. [Guidelines and Account Authorization, Kansas State University]

2.3.3 Device Security

- CSANZ acquiesce to the increasing use of personal devices for work purposes. Use of personal devices for work purposes requires prior approval from the ICT department to ensure security compliance. [Bring Your Own Device (BYOD) Policy Considerations for Federal Information Systems and Organizations, NIST SP 800-161]

- To guarantee system security and compatibility, CSANZ members should forbear from installing unauthorized software on organizational devices. IT staff will manage the installation and updates of all necessary software. [Security and Privacy Controls for Federal Information Systems and Organizations (FISMA), NIST Special Publication (SP) 800-53, Revision 5]

- CSANZ prioritizes the security of our members' and collaborators' devices. To achieve this, Endpoint Detection and Response (EDR) solutions are leveraged. [CrowdStrike EDR]

- CSANZ notice that when on public Wi-Fi, members and collaborators must steer clear of accessing sensitive information or organizational accounts. If it is of necessity for them then they must use a secure Virtual Private Network (VPN) to build a further layer of security. [Cyber Supply Chain Risk Management, NIST Special Publication (SP) 800-161, Revision 1]

2.3.4 Data Security

- CSANZ partake of regular penetration testing to flag vulnerabilities in the systems and infrastructure. CSANZ keep up vulnerability management programs to underscore and correct picked security weaknesses. [An Introduction to Information Security, NIST Special Publication (SP) 800-12, Revision 1]

- CSANZ order members and collaborators to use of Multi-Factor Authentication (MFA) for their accounts. [NIST Small Business Cyber Security Fact Sheet, Multi-Factor Authentication]
- Industry-standard encryption algorithms are enacted by CSANZ to watch over delicate data in storage as well as while being transferred. [International Organization for Standardization (ISO) 27001]
- CSANZ also encrypt sensitive data when sending emails outside the organization. [Health Insurance Portability and Accountability Act (HIPAA) Security Rule 45 CFR § 164.308(a)(1)(ii)(A)]
- Zero Trust security model is endorsed by CSANZ, where all members and collaborators, and their devices must be continuously authenticated and authorized before accessing any resources which eliminates implicit trust and minimizes the attack surface [Zero Trust: The What, Why And How]

2.3.5 Communication and Monitoring

- All electronic communication channels, including email and social media, should show CSANZ's adherence to professionalism.[Society for Human Resource Management (SHRM) Social Media Guidelines, 2023]
- CSANZ take in a safe cloud-based communication platform (e.g., Microsoft Teams, Slack) for internal communication and collaboration which give the means to methodical information sharing, project discussions, and real-time correspondence among CSANZ members[The CISO Guide to Cloud Communications Security]
- CSANZ fort key data with a robust DLP solution which surveils and bars the handover of sensitive data via email, file downloads, or cloud storage. [New Gartner Report on data loss prevention]
- CSANZ book the right to archive and monitor work-related electronic communications, including emails, instant messages, and voicemails, to make sure cooperativeness with legal regulations, conduct investigations, and evaluate employee performance. While CSANZ respect the justifiable expectation of privacy for personal communications on organizational equipment, this expectation is limited for work-related messages. [Electronic Communications Privacy Act (ECPA) of 1986, 18 U.S.C. § 2701 et seq.]

2.4 Review and Updates

CSANZ is dutiful in prolonging a dynamic and effective ICT policy. This policy will be reviewed and updated periodically to ensure the evolving landscape of technology, legislation, and best practices.

2.5 Consequences of Non-Compliance

Contravention with this ICT policy will call for disciplinary actions, which may extend from a simple reminder to more serious results. CSANZ saves the right to seek after lawful action within the occasion of policy breach.

2.6 Disclaimer

Root fundamentals for mindful utilization of CSANZ's information and communication innovation assets are laid out by this ICT arrangement. It serves as a foundational system and may be extended upon with extra rules as required

2.7 Conclusion

By grasping this ICT Policy, we collectively cultivate a secure and beneficial work environment for all CSANZ members and collaborators. This approach guarantees the security of important data depended to us. For advance request, if you don't mind do not delay contacting the ICT division.

.

References

Damalouji, T. B., Lillia. (2023, October). Two New Cybersecurity Proposed Rules Mean Big Changes for Federal Contractors. Retrieved March 25, 2024, from https://www.governmentcontractslawblog.com/2023/10/articles/cybersecurity/two-new-cybersecurity-proposed-rules-mean-big-changes-for-federal-contractors/

Data Privacy Day 2024 – Key Global Developments in Data Privacy and Cybersecurity in 2023 and What to Expect in 2024. (2024). Retrieved March 25, 2024, from https://www-upgrade.cov.com/en/news-and-insights/insights/2024/01/data-privacy-day-2024-key-global-developments-in-data-privacy-and-cybersecurity-in-2023-and-what-to-expect-in-2024

Davies, A. (2021). COVID-19 and ICT-Supported Remote Working: Opportunities for Rural Economies [Number: 1 Publisher: Multidisciplinary Digital Publishing Institute]. World, 2(1), 139–152. https://doi.org/10.3390/world2010010

Impact of COVID-19 on the use of ICT in enterprises. (2022). Retrieved March 25, 2024, from https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Impact_of_COVID-19_on_the_use_of_ICT_in_enterprises

The pandemic has boosted firm investments in digital technologies. (2021, August). Retrieved March 25, 2024, from https://cepr.org/voxeu/columns/pandemic-has-boosted-firm-investments-digital-technologies

Ponder. (2023). U.S. Tech Legislative & Regulatory Update – Second Quarter 2023. Inside Privacy. https://www.insideprivacy.com/technology/u-s-tech-legislative-regulatory-update-second-quarter-2023/

SEC Issues New Requirements for Cybersecurity Disclosures. (2023). Retrieved March 25, 2024, from https://dart.deloitte.com/publications/deloitte/heads-up/2023/sec-rule-cyber-disclosures

Seven lessons learned about digital security during the COVID-19 crisis. (2020). Retrieved March 25, 2024, from https://www.oecd.org/coronavirus/policy-responses/seven-lessons-learned-about-digital-security-during-the-covid-19-crisis-e55a6b9a/

Yang, S., Fichman, P., Zhu, X., Sanfilippo, M., Li, S., & Fleischmann, K. R. (2020). The use of ICT during COVID-19. Proceedings of the Association for Information Science and Techn 57(1), e297. https://doi.org/10.1002/pra2.297