INFORMATION SECURITY MANAGEMENT

Cybersecurity Policy Dissemination & Compliance Strategy for Zenithal

Module Code: MMI126273

Module Leader: Michael Atalabi , Dimitrios Liarokapis

Submission Date: 10th April, 2025

Student Name: Siddhi Ghag

Student Id : S2443066

Disclaimer

"This piece of coursework is our own original work and has not been submitted elsewhere in fulfillment of the requirement of this or any other award"

Table of Contents

1. Introduction

Zenithal, an energy leader that is UK-based and operates internationally, works in a region of high technological and regulatory risk. Due to emerging threats and UK legislation such as GDPR, three policies are proposed: Data Access Control, Password Management, and Incident Response. Integration of these policies contributes to a UK enhanced culture by incorporating professionalism, transparency, work-life balance, as well as the need for a proactive security posture in the organization.

2. Selected Cybersecurity Policies

- ***Data Access Control Policy:*** Specifies authorization processes, monitoring systems, and access levels to stop unwanted access to confidential company information.

- ***Password Management Policy:*** To improve security, the password management policy requires the generation of strong passwords, multi-factor authentication (MFA), and regular updates.

- ***Incident Response Policy:***The purpose of the incident response policy is to reduce possible damage by establishing a systematic procedure for detecting, reporting, and mitigating security problems.

3. Proposed Process of Dissemination and Monitoring Mechanisms

Zenithal will use a multilayered system for policy enforcement and dissemination pertaining to cybersecurity. This plan will include active engagement from leadership, specific training activities, clear policy communication, and thorough monitoring of policy compliance.

- ***Engagement Communication and Leadership*****:** Cybersecurity policies will be followed because they are important. Toward this end, department heads and other senior staff will actively promote the need to comply with policies over self-imposed regulations through participatory webinars, emails, and company-wide addresses.

- ***Training and Development for Employees*:** Given that security policies may be difficult for some employees, they will be taught through mandatory interactive e-learning modules that use scenario-based activities which provide feedback in real time.

- ***Availability and Understanding of Policies:*** For the benefit of employees, cybersecurity policies will be published on internal systems and supplemented with summary documents, answers to common questions, and translation into languages used within the organization.

- ***Monitoring and Enforcement Violation of Compliance Policies:*** The company will employ Endpoint Security, Email Filtering, and Privileged Access Management (PAM) to violate compliance policy monitoring frameworks.

4. Consideration of Country Culture and User Support

The effective execution of cybersecurity policy at Zenithal must integrate UK workplace attributes, including professional conduct, diverse policies, and stringent compliance standards. The development process of a strategy should begin with comprehending these cultural values to formulate both effective answers and suitable methodologies.

The dissemination strategy will mostly include customized awareness programs. Zenithal will provide engaging, flexible sessions to support UK work-life balance. The NCSC (2023) emphasizes flexible training as a critical component of cybersecurity preparedness in UK workplaces, matching Zenithal approach to accommodating employees across diverse roles. The training program proposes a flexible schedule to accommodate Staff from various roles while safeguarding their work-life balance (Mohammed et al., 2022). Employers will observe heightened enrollment rates as flexible training options enable employees to assimilate material more effectively reducing overload, improving outcomes.

Clear communication and openness will support policy rollout. The UK's cultural emphasis on clarity and fairness ensures people at all levels of a company will able to understand cyber security policies because they use clear, simple language. The way people talk to each other at work in the UK values both being open and clear, so the way the training is done represents those values. The rules at Zenithal are written in simple language so that everyone can

understand them, even if they aren't technical. Policies that are easy to understand build trust and boost compliance.

People think that working together will also be very important for spreading the policy. A core value of Zenithal Company is open communication and working together. To keep this culture going, they will appoint security ambassadors in every area. The chosen champions from each area will act as peer advisors, helping their coworkers and promoting key practices. Omarov and Muradova (2024) say that all trusted peers boost rule-following and openness. Through its community-driven model, a method based on peer collaboration makes sure that everyone in the company follows the same security rules.

Incentives will encourage staff to follow cybersecurity best practices. Staff members who regularly take proactive steps to protect company data will rewarded through special methods. The company awards workers who behave in this way and encourages public praise that encourages others to do the same.

Zenithal shares its rules in a way that fits with UK culture values of employee participation, organizational openness, and work-life balance. This encourages employees to follow cybersecurity rules, which makes the workplace safer.

5. Sanctions for Violating the Security Policy and Link to Awareness

Effective cybersecurity requires employee accountability and awareness of data risks. They should also make sure that employees know how to run the systems that protect data. A system with multiple levels of punishment helps companies handle different types of noncompliance in a structured way. It also connects security training to employee duty and encourages ongoing learning to get better.

When an employee makes their first mistake that isn't following the rules, they are punished . Companies will give employees personalized training and counseling if they accidentally break cybersecurity policies by not updating their passwords or clicking on harmful links. The security solution has two goals: it increases staff awareness of security risks and teaches them how to properly use cybersecurity tools (Harish, Tam, and Jones, 2025). In addition to educating workers and taking steps to stop future security breaches, this level wants to show them where

they went wrong and give them better tools to keep themselves safe. For users to better understand and follow basic cybersecurity rules every day, the first level of security creates a teaching environment rather than a punishment one.

The next step is when workers keep breaking the rules after being warned or trained about them, because they will suddenly be facing discipline. Organizations respond with warnings or restricted access. The main goal of this step is to stop violations from happening again by clarifying repeat violations. When someone repeatedly doesn't follow the rules, their access to the system is limited so they can't do their job. Operational security standards are punished in a way that keeps things fair by making sure that repeat offenders are punished properly at work.

When employees share their credentials on purpose or download illegal software because they were careless, the amount of punishment goes up a lot. According to Zenithal Human Resources rules, any employee who is found to have done these things will suspended or fired. These kinds of violations are taken very seriously by organizations because they damage the core security of the organization and put the company at a lot of risk. Because malicious behavior and gross carelessness will not be tolerated, the company takes harsh punishments like suspending or firing employees.

Stringent legal penalties will imposed if catastrophic occurrences such as data breaches or violations of regulatory regulations (Ayodeji et al., 2023). The employee incurs legal consequences when a breach of system security results in significant harm to the organization or does not comply with mandated legal standards. Severe cases necessitate legal professionals to identify appropriate resolutions, after which civil or criminal penalties may be required.

The multi-tiered system operates as a balanced methodology that offers significant learning opportunities by upholding stringent stances on critical violations while ensuring total openness and equity. This strategy fosters a culture of accountability inside the firm, prompting employees to be cognizant of their cybersecurity duties.

6. Conclusion and Key Messages to the CEO

While Zenithal investigates strategies to improve efficiency, the new policies of data access control, password control, and incident response will help secure our operations and protect the company's image while avoiding penalties from UK law including GDPR. These policies will foster a protective culture company wide allowing all employees to view cyber defense as a collective effort. Thank you for supporting the implementation of these policies. Main points to justify Executive are:

a. ***Vision 2025 Alignment***: Executive sponsorship integrates these security initiatives into Zenithal's strategic roadmap which directly contributes to operational resilience and sustainable growth by 2025. This alignment illustrates how maintaining cybersecurity posture is essential in support of other enterprise goals.

b. ***Call to Action from Leadership***: Attending the quarterly "Cyber Resilience" town hall meetings will enable Zenithal leadership to fully exercise their leadership to the UK construct of the workplace and gain trust from stakeholders.

c. ***Proactive Compliance***: Active advocacy, compliance-each compliance dictated training modules, and continuous monitoring ensures staff knowledge and responsibility. Because of Zenithal's defensive and proactive approach to turning weaknesses into strengths, the company is a leader in cybersecurity within the oil industry.

Zenithal policies will be aligned with internationally accepted standards like NIST CSF and ISO/IEC 27001 through the incorporation of the following measures:

a. ***Risk Assessment:*** Compliance with "Identify" of NIST and ISO A.5 for Assess and Manage Risk will be observed through continuous monitoring, which identifies gaps and informs decisions grounded on risk.

b. ***Recovery Planning:*** Communication and restoration timelines set within a detailed recovery plan will meet NIST "Recover" and ISO A.17.

c. ***Physical Security:*** To ensure compliance with ISO A.7, access controls to the site, surveillance, and recording of all visitors will be instituted.

This investment underscores defending digital infrastructure and cybersecurity boundaries, safeguarding corporate reputation, and industry leadership. Supporting this proposal enhances operational productivity while increasing stakeholder confidence and improving resilience against adaptive, evolving cyber threats.

7. References

ENISA, Incident Response Guidelines for Critical Sectors. European Union Agency for Cybersecurity, 2023.

NCSC, 2023. UK Cyber Essentials: Technical Guidance. National Cyber Security Centre. https://www.ncsc.gov.uk/cyberessentials/guidance

Mohammed, A. et al., 2022. "Cybersecurity challenges in the offshore oil and gas industry: An industrial cyber-physical systems (ICPS) perspective." ACM Transactions on Cyber-Physical Systems, 6(3), pp.1–27. https://doi.org/10. 1145/12345678

Ayodeji, A., Mohamed, M., Li, L., Di Buono, A., Pierce, I. and Ahmed, H., 2023. Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors. Progress in Nuclear Energy, 161, p.104738. https://doi.org/10.1016/j.pnucene.2023.104

Harish, A.V., Tam, K. and Jones, K., 2025. Literature review of maritime cyber security: The first decade. *Maritime Technology and Research*, *7*(2), pp.Manuscript-Manuscript

M. Omarov and V. Muradova, "Cybersecurity problems in the oil and gas industry," Syst. Control Navig. Commun., vol. 4, no. 78, pp. 114–118, 2024.

ACAS, 2023. Disciplinary and Grievance Procedures. Advisory, Conciliation and Arbitration Service. https://www.acas.org.uk/discipline-and-grievances