Project Part 1:

Security Governance and Compliance

Justin Langevin

8648380

Conestoga College

SECU74020:

Secure Enterprise Architecture

July 28, 2024

Security Policies Document

Data protection policy

- Data Classification
    - All data must be classified based on its sensitivity.
- Data Encryption
    - All sensitive data must be encrypted at rest and in transit using AES-256.
- Data Access
    - Data Access must be restricted using the principle of least privilege.
- Data Backup
    - Regular backups are required and backup data must be encrypted and stored securely.
- Data Disposal
    - Secure data disposal methods must be used for sensitive data.

User Access Management Policy

- User Authentication
    - Multi-factor Authentication will be used for accessing sensitive systems.
- Access Control
    - Role-based access controls (RBAC) must be used to ensure users only have access to necessary resources based on their role.
- User Provisioning
    - New users and their accounts must be approved by the user manager and IT department.
- User De-Provisioning

    - All user accounts must be promptly deactivated when the employee leaves the organization or when no longer needed.
- Access Review
    - All user access rights must be regularly reviewed.

Incident Response

- Incident Detection
    - All systems must have logs that are monitored to ensure the detection of security incidents.
- Incident Reporting
    - All security incidents must be reported to the security team.
- Incident Response Team
    - An Incident Response Team (IRT) must be established this team includes IT/Infra, Legal, HR/Public Relations, Cyber, and DFIR.
- Incident Handling
    - The IRT must follow a defined incident response plan which includes identification, containment, eradication, recovery, and a lessons learned section.
- Post-Incident Review
    - The incident must be reviewed to help identify any improvement and update any policies or procedures that can be improved.

Compliance Mapping Report

Data Protection Policy

- Compliance Standards

    - GDPR, HIPAA, ISO/IEC 27001

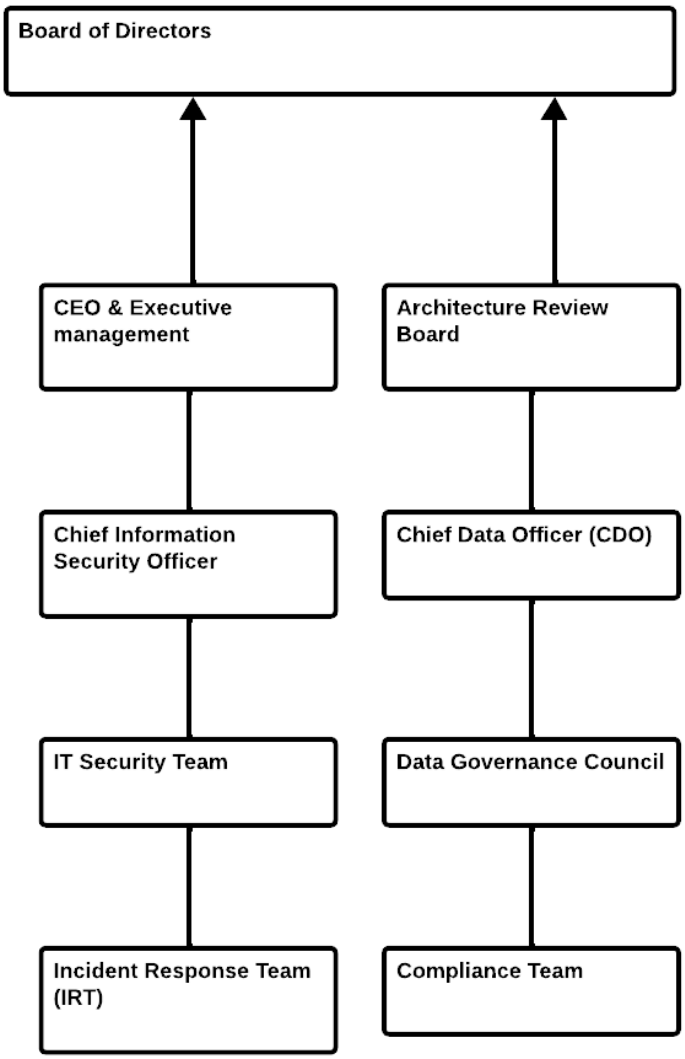
User Access Management Policy

- Compliance Standards
    - ISO/IEC 27001, NIST SP 800-53

Incident Response Policy

- ISO/IEC 27001, NIST SP 800-61

Governance Framework Diagram



References

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *Computer Security Incident Handling Guide*, *2*(2). https://doi.org/10.6028/nist.sp.800-61r2

CISCO. (n.d.). *Networking, Cloud, and Cybersecurity Solutions*. Cisco. https://www.cisco.com/site/ca/en/index.html

CrowdStrike. (n.d.). *The CrowdStrike Falcon® platform*. Crowdstrike.com. https://www.crowdstrike.com/platform/

Fortinet. (2023). *Next-Generation Firewall (NGFW)*. Fortinet. https://www.fortinet.com/products/next-generation-firewall

ISO. (2023). *ISO/IEC 27001:2022(en)*. Iso.org. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

NIST. (2020). Security and privacy controls for information systems and organizations. *Security and Privacy Controlsfor Information Systems and Organizations*, *5*(5). https://doi.org/10.6028/nist.sp.800-53r5

paloalto networks. (n.d.). *Global Cybersecurity Leader - Palo Alto Networks*. Www.paloaltonetworks.com. https://www.paloaltonetworks.com/

rockwell. (n.d.). *MES Solutions for Life Sciences | FactoryTalk | US*. Rockwell Automation. Retrieved July 25, 2024, from https://www.rockwellautomation.com/en-ca/products/software/factorytalk/operationsuite/mes/life-sciences.html

SAP. (n.d.). *MES: The Power of Real-Time Data*. SAP. https://www.sap.com/canada/products/scm/execution-mes/what-is-mes.html

SOLARWINDS. (n.d.). *What Is WSUS? Windows Server Update Services Guide - IT Glossary | SolarWinds*. Www.solarwinds.com. https://www.solarwinds.com/resources/it-glossary/wsus-windows-server-update-services