CYBERSECURITY POLICIES AND RISK MANAGEMENT

ASSIGNMENT-2

ASSET MANAGEMENT POLICY

STUDENT NAME : AKSHATHA SAI PASHAM

STUDENT ID : 700759936

PROFESSOR : DR. RICHARD MORPHY

Asset Management Policy of Shallow Cosmos Tech

Purpose

This policy is designed to establish the principles and procedures that dictate asset management decisions at Shallow Cosmos Tech, aiming to uphold Shallow Cosmos's mission of delivering top-notch products with a sustainable and secure framework. This policy essentially acts as a rulebook for handling backup resources within the organization. It covers everything involved in backing up and recovering data, including the systems, devices, and infrastructure used for the process.

Scope

This Asset Management Policy is relevant to every asset under the ownership of Shallow Cosmos, encompassing all stages of each asset's lifecycle, such as design, construction, operation, maintenance, and disposal. It is applicable to all personnel, including employees, contractors, and consultants affiliated with Shallow Cosmos. Furthermore, Shallow Cosmos may depend on assets, including natural or non-owned assets. In cases where these assets support operation, we will engage in cooperative efforts with the asset proprietors and advocate for the principles articulated in this policy.

Policy

Backup

- **Management of backup systems**

• To adhere to organizational standards, it is essential to obtain backup systems and storage devices from approved vendors and configure them accordingly.
• When installing backup systems, follow the manufacturer's recommendations and instructions carefully and adhere to recognized best practices in the field.(CP-9, 2023)
• To guarantee the accuracy and accessibility of important data, establish and execute regular backup schedules.
• Implement consistent maintenance and update routines for backup systems to close security gaps and optimize performance.(Barrett M., 2018)
• To ensure continued data privacy, securely dispose of backup hardware and media nearing the end of their lifespan.

- **Documentation**

• Backup assets like hardware, software and storage media must be documented and maintained in a centralized inventory.(CP-11,12, 2023)
• The documentation must be detailed including specifications, configurations and maintenance history.

- **Monitoring of backup**

- Proactively monitor backup systems for performance, errors and any unexpected behavior. The logs of backup operations must be regularly viewed to verify successful completion and detect potential problems.(CP-14, 2023)

- **Risk Assessment**
- Risk assessment includes the scheduling of regular checkups for backup dangers or risks and fixing them beforehand.(ID.RA, ID.PT, ID.DP, 2020)
- Plan out a response or recovery for when the backup fails or when there occurs a data loss. (ID.RP, ID.RE, 2020)

- **Auditing**
- Regular audits must be conducted to assess the compliance with the backup policies and guidelines(ID.BE, CSF2020). The backup inventory also must comply with the industry regulations.(CP-12,13, 2023)

- **Awareness**
- Workshops must be conducted for the IT Staff inorder to make them aware of the backup procedures and tools.

Mapped Controls

- NIST SP 800-53v5 Controls
- CP-9 - Information System Backup
- CP-10 - Information System Recovery and Reconstitution
- CP-11 - Alternate Storage Site
- CP-12 - Backup Storage Capacity
- CP-13 - Backup Integrity
- CP-14 - Testing and Exercise

- Cybersecurity Framework (CSF)
- ID.RA - Risk Assessment
- ID.BE - Business Environment
- ID.PT - Protect
- ID.DP - Detect
- ID.RP - Respond
- ID.RE - Recover

References

- Barrett, M.,Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework, (2018), https://doi.org/10.6028/NIST.CSWP.04162018
- National Institute of Standards and Technology. (2020). Cybersecurity Framework (CSF). https://www.nist.gov/cyberframework

• National Institute of Standards and Technology. (2023). Security and Privacy Controls for Information Systems and Organizations (Special Publication 800-53v5). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf