

CYBERSECURITY POLICY AND RISK MANAGEMENT

ASSIGNMENT-1

ACCEPTABLE USE POLICY

STUDENT NAME : AKSHATHA SAI PASHAM

STUDENT ID : 700759936

PROFESSOR : DR. RICHARD MORPHY

Acceptable Use Policy Of Shallow Cosmos Tech

Purpose

The purpose of the Shallow Cosmos Tech Acceptable Use Policy is to establish acceptable practices regarding the use of the company's Information Resources in order to protect the confidentiality, integrity and availability of the information created and being recorded. This helps ensure the security and proper use of confidential and sensitive information. This Acceptable Use Policy defines the acceptable and unacceptable behaviors of the personnel using Shallow Cosmos Tech's information technology resources.

Audience

The Acceptable Use Policy of Shallow Cosmos Tech is applicable to any person, organization, or procedure that engages with any Information Resource provided by the company.

Policy

Unauthorized Access to the Company Computers

Shallow Cosmos Tech takes computer security seriously. This policy is crucial to the organization as information security breaches have gained an unprecedented potential to impact negatively on businesses' reputation, profitability, customer confidence and overall economic growth. It forbids any unauthorized access to computer systems. This includes computer networks, systems, and resources of any kind. Any attempt to gain access without obtaining prior authorization is a serious violation and may result in significant consequences.

CSF Section and Sub-Category

- Identify (ID)

Access Control (AC)

Related 800-53v5 Controls

- AC-1: Access Control Policy and Procedures
- AC-2: Account Management
- AC-3: Access Enforcement

Unauthorized Access to Company Data

Safeguarding the company's data security and privacy is very crucial to Shallow Cosmos Tech. Stored data sometimes have personal or social values that become lost when the data are corrupted, causing

psychological or emotional harm. Personnel are prohibited from accessing and altering the company data without appropriate authorization. Great importance is given on upholding the confidentiality and integrity of data. Data is to be encrypted at rest and in transit. The use of firewalls and Intrusion detection and prevention systems are crucial in avoiding unauthorized access to data. Data breaches are to be prevented in order to uphold the organization's reputation, financial stability and competitive advantage. Consumers and employees need to be able to trust that their data is safe within Shallow Cosmos Tech.

CSF Section and Sub-Category

- Protect (PR)
- Data Security (DS)

Related 800-53v5 Controls

- AC-6: Least Privilege
- AC-8: System Use Notification

Equipment must be kept safe

Shallow Cosmos Tech expects personnel to be responsible for their own devices - laptops, phones etc. This includes protecting them from physical damage, loss and theft. To enhance security, the use of strong passwords, encryption of sensitive data and updating of software must be done. Shallow Cosmos Tech does not actively monitor communications i.e emails, chats, on the network. This means active check for compliance with policies and laws is not done. However, the systems might passively pick up on suspicious activity during regular network maintenance. Protecting personnel's own data helps in maintaining a secure environment within the organization.

CSF Section and Sub-Category

- Respond (RS)
- Response Planning (RP)

Related 800-53v5 Controls

- CP-2: Contingency Planning
- CP-9: Information System Backup

Content Exploration Restrictions

Shallow Cosmos Tech imposes restrictions on certain content categories that the personnel can browse through. These include pornography, military-related material, gambling and internet shopping. The purpose behind these restrictions is to maintain a safe and appropriate environment in alignment with

the company's principles, and legal considerations. The organization will make sure that the IT staff periodically reviews and updates this policy and document the changes in revision tables. This policy gives Shallow Cosmos Tech the right to modify or withdraw this policy at any time given the necessity. But this can be done after promptly informing the employees all updates.

CSF Section and Sub-Category

- Identify (ID)
- Asset Management (AM)

Related 800-53v5 Controls

- AC-4: Information Flow Enforcement
- AC-19: Access Control for Mobile Devices

References

- Dlamini, M., Eloff, J. H. P., & Eloff, M. M. (2009).
 - Information security: The moving target. *Computers & Security*, 28(3–4), 189–198.
 - <https://doi.org/10.1016/j.cose.2008.11.007>
- Wen-Lung Shiau, Xiaoqun Wang, Fei Zheng (2023).
 - What are the trend and core knowledge of information security? A citation and co-citation analysis?
 - <https://www.sciencedirect.com/science/article/abs/pii/S0378720623000228>
- D'Arcy, J., Hovav, A., & Galletta, D. F. (2009).
 - User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence approach. *Information Systems Research*, 20(1), 79–98.
 - <https://doi.org/10.1287/isre.1070.0160>
- CSF Tools. (2023, December 23).
 - *Acceptable use of Technology Policy and Procedures - CSF tools*. CSF Tools - the Cybersecurity Framework for Humans.
 - <https://csf.tools/reference/cloud-controls-matrix/v4-0/hrs/hrs-02/>

