# Unit 3 Assignment - Creating an Operational Security Plan and Policy

# Amon-Ra

# Herzing University

BU622 Information Security and Privacy

1. **Purpose**

The purpose of the Operational Security Plan and Policy is to safeguard company hardware, software, and data from internal and external threats in accordance with International Organization for Standardization (ISO) 27002. A risk assessment conducted by the company has revealed internal and external risks to the organization’s information technology assets that need to be addressed.

1. **Scope**

This policy applies to all employees, contract employees, interns and all other visitors and all company hardware, software, data, and its premises.

1. **Responsibility**

The Technology Director will be responsible for the implementation of the Operational Security Plan and Policy.

1. **Policy**

# The ensure business continuity of Zanzibar Spice, LLC, the Operational Security Plan and Policy helps to identify threats and vulnerabilities and implement controls to reduce the overall risk to information technology assets. The following policy is defined as the Operational Security Plan to safeguard company assets:

* 1. Physical access to the information technology room will be controlled and under and key.
  2. The information technology room will be under recorded surveillance 24 hours a day, 7 days a week.
  3. Servers will be stored in a rack having a cage barrier, key and lock.
  4. Network equipment stored in a rack having a cage barrier, key and lock.
  5. Employee permissions to data shall have minimum privileges necessary to perform their responsibilities.
  6. Data will be backed up daily.
  7. Server software will be maintained and updated promptly as patches/updates are released by the vendor.
  8. Antivirus software will be installed and maintained on company servers.
  9. Servers will have adequate processing.
  10. Servers will have adequate storage capacity.
  11. Company laptops will have antivirus software installed on them and maintained.
  12. Company laptops hard drives encrypted.
  13. Company laptops ability to use external storage devices will be disabled.
  14. Firewalls will be maintained in a manner to deny access to unauthorized access and permit authorized access to the company information technology infrastructure.
  15. Power redundancy for server equipment will be implemented and maintained.
  16. Power redundancy for network equipment will be implemented and maintained.
  17. Company internet access will be redundant.
  18. Company internet access will have adequate bandwidth.
  19. Company internet access will have protection against DDOS attacks.

1. **Enforcement**

Violation of this policy may be subjected to disciplinary, criminal, and/or civil penalties.

1. **Revision History**

|  |  |  |
| --- | --- | --- |
| Date of Change | Executor of Change | Summary of Change |
| 07/26/2020 | Amon-Ra | Creation |

References:

Biswas, Pretesh. (2020 Feb 1). Example of Physical Security Policy (Links to an external site.). https://isoconsultantkuwait.com/2020/02/01/example-of-physical-security-policy/

Information Security Plan Policy. (n.d.). Retrieved July 26, 2020, from http://www.ccis.edu/policies/information-security-plan-policy.aspx

Security Operations Policy. (n.d.). Retrieved July 26, 2020, from https://www.pomona.edu/sites/default/files/its-security-operations-policy.pdf

Security Policy Templates (Links to an external site.). (n.d.). SANS. https://www.sans.org/information-security-policy/