Security +
Corporate Policy

Author: Joseph Lee
Email: joseph@ripplesoftware.ca
Mobile: 778-725-3206

General Terms

SOA Standard Operating Procedures
- Provide step by step instructions for employees on how to perform tasks or operations

AUP Acceptable Use Policy
- Defines proper system usages and rules of behaviour for employees when using resources

Privacy Policy Statement
- Outlines the organizations privacy policy to set the user / employees expectations for privacy

Mobile Device Deployment Models

Corporate owned
- Organization purchases devices and issues them to employees

COPE Corporate Owned Personal Enabled
- Same as corporate owned, but employees are allowed to use he device for personal use

BYOD Bring your own device
- Employee brings their own device

CYOD Choose your own device
- Organization buys the device of your choice from a set list of supported devices
- Allows a specific list of devices that administration can support, monitor and manage

Educating Users

- Untrained users are perhaps the biggest risk to an organization
- Insiders even though not malicious are a gateway to the IT infrastructure inside the network
- Clicking on a link in a malicious email could allow malicious code to run on internal network resources

- Members of the organization may be unaware of attacker’s methods
- Some methods of increasing awareness can include:
  - Formal classes
  - Requiring certification
  - Online courses
  - Signage
  - Newsletters / Bulletin
  - Website banners / warning messages / pop-ups
  - Informative Emails
  - Trend alerts (phishing warnings, zero-day exploits, malware, hoax)
  - Meetings

Agreement Types

BPA Business Partners Agreement

- A written agreement that details the relationship between business partners, including their obligations towards the partnership
- It is a business contract that stipulates profit sharing, and conditions of ending the partnership

SLA Service Level Agreement

- Stipulates performance expectations of services such as minimum uptime requirements
- SLAs are used when contracting services from service providers such as ISP
- Many SLA includes monetary penalties when requirement are not met

ISA Interconnection Security Agreement

- Specifies technical and security requirements for connecting two or more entities
- It may stipulate minimum security requirements for data-in-transit and/or data-at-rest

MOU/MOA Memorandum of Understanding or Memorandum of Agreement

- Expresses understanding between to or more parties indicating intentions to work towards a goal
- MOA/MOU often support an ISA by defining the purpose of the ISA

Personnel Management

Mandatory vacations

- Used as a time when a position can be reviewed to detect fraud, embezzlement, etc.

Separation of duties

- Prevents a single person or entity from being able to complete all the functions of a critical or sensitive process

- Can prevent fraud, theft, errors, corruption
- In development, this principle can be used to prevent malware from being added to software by separating the development, testing, and production teams

Job Rotation
- Helps prevent dangerous short-cuts or fraud by allowing multiple people to review work in that position
- People keep an eye on each other

Clean desk policy
- Prevents data loss by exposing sensitive data and items such as keys, cellphones, access cards, papers, passwords, files, PII, etc.

Background checks
- Checking criminal background, references from previous employers, credit history, etc.

NDA Non-disclosure agreement
- Used to attempt to prevent proprietary data is not disclosed

Exit Interview
- Conducted with departing employees who have quit or fired
- Some common questions help understand their position on the job and may allow changes to the job in the future

On-boarding
- The process associated with hiring a new employee
- These processes include granting access, and creating accounts such as network accounts, email, etc.
- Also, on-boarding will familiarize the new employee with agreements and policies of the organization

Off-boarding
- The process of removing access to accounts and disabling, or archieving the accounts