Network Security Policy Guidelines

Jon Misevicz

Contents

[ ACCEPTABLE USE POLICY 3](#_Toc386997454)

[ USER ACCOUNT MANAGEMENT POLICY 3](#_Toc386997455)

[ NETWORK ACCESS POLICY 4](#_Toc386997456)

[ INTERNET USE POLICY 4](#_Toc386997457)

[ SERVER AND DESKTOP POLICY 5](#_Toc386997458)

[ SOFTWARE LICENSING POLICY 5](#_Toc386997459)

[ MOBILE DEVICES POLICY 6](#_Toc386997460)

[ REMOTE ACCESS POLICY 6](#_Toc386997461)

[ GUEST ACCESS POLICY 6](#_Toc386997462)

[ MALWARE POLICY 6](#_Toc386997463)

[ CHANGE MANAGEMENT POLICY 7](#_Toc386997464)

* ACCEPTABLE USE POLICY
	+ Company XYZ reserves the right, at their discretion, to monitor, and record any and all activities which use, but are not limited to, the company’s hardware and communication infrastructure.
	+ There is no reasonable expectation of privacy when using company property to facilitate communications.
	+ As an employee of company XYZ, I will follow the following security rules:
		- I will not try to access restricted files, nor will I install programs which have not been authorized prior.
		- I will not protect my user credentials including password, and I understand that I can be held liable for any and all activity when logged into the network.
		- I will not download, or use cloud enabled file sharing software. Any large file transfers will be done though the corporate FTP site, or an approved third party.
		- I will limit my use of social networks, including instant messaging, to break or lunch hours. Excessive use will be recorded and management will be notified
		- I will not participate in any activities that are considered illegal under local, state or federal laws while using company infrastructure.
		- I will not store copyrighted material on company file shares, local computers or access third party cloud storage.
		- I understand that these rules are not exhaustive and are meant to provide a guiding framework.
	+ Unauthorized encryption software is not allowed when dealing with company resources and proprietary data.
* USER ACCOUNT MANAGEMENT POLICY
	+ Each employee is assigned a unique network identity which will be used to audit activities using company resources.
	+ New user privileges will be assigned by Information Management under department management guidelines. A user will only be assigned the minimum security needed to carry out their assigned duties.
	+ If an employee requires additional privileges, the notification is required to be sent from their assigned supervisor or manager to Information Management with appropriate justification including reasonable time limit for elevated permissions.
	+ Information Management will record and manage all requests in compliance with state, federal and corporate guidelines.
	+ At no one time will any privileged or super user account be authorized without the consent of the manager of Information Management and another member of the leadership team.
	+ Annual audit of user permissions will be carried out by Information Management with results submitted to the leadership team for review and possible implementation.
	+ All credentials for terminated or suspended employees will be disabled and requires notification from Human Resources for reactivation. Information Management cannot reactivate a terminated employee without prior authorization.
	+ User account passwords will expire 60 days from initial creation. Password requirements are as such:
		- Longer than 8 characters
		- Contain upper and lower case characters
		- Contain at least one number and symbol
		- Cannot be similar to previous 10 passwords
		- Cannot contain username
		- Cannot contain consecutive characters nor numbered sequences.
* NETWORK ACCESS POLICY
	+ The network infrastructure is to be used by employees while on company time. Access to corporate resources is authorized to conduct business.
	+ Accounts for guest access is detailed in the guest account sections.
	+ Any client or user that is found in violation of this policy, or at the discretion of Information Management, maybe be denied access to network resources.
	+ Any attempt to gain unauthorized access to network devices will be reported, including, but not limited to:
		- Tampering with network devices such as access point, router, or switch.
		- Aiding in unauthorized personnel accessing a secure area which is normally locked.
		- Participating in an unauthorized activity that places an unneeded load onto network resources.
* INTERNET USE POLICY
	+ Internet use is granted primarily for use during the normal course of business. Limited personal use is authorized.
	+ Employees will not use the company’s internet access to access:
		- Abusive, vulgar, threatening, racist or explicit language
		- Obscene, pornographic or sexual material.
		- Information which advocates violence or discrimination toward people, or that constitutes harassment.
		- The transfer of copyrighted material or unauthorized proprietary information.
		- No posting onto social media sites any information which could be considered detrimental to the company’s image.
	+ Employees will not use company internet resources to transmit unsolicited email or SPAM.
	+ The company reserves the right to limit, without notification, any site it deems inappropriate.
* SERVER AND DESKTOP POLICY
	+ Servers
		- Only employees authorized by Information Management shall be granted access to the physical servers, or console.
		- All access to privileged accounts outside of designated employees shall be logged.
		- Servers will only be housed in an area where the physical access can be controlled.
		- Unused applications or services will be disabled.
		- Servers which house services which are accessed from outside the network shall be connected within the Demilitarized Network Zone to comply with segregation in line with best security practices.
	+ Desktop/Laptop.
		- All security related events will be logged and reported.
		- Laptop computers will be encrypted using a network security policy.
		- Lost or stolen laptops will be reported immediately to so that appropriate actions may be taken such as erasing of hard drive remotely.
		- All desktops will be set to auto lock after 5 minutes of idle time.
		- Any desktop or laptop may be scanned at any time without employee notification.
* SOFTWARE LICENSING POLICY
	+ Software license agreements shall be maintained within Information Management Department to assure compliances with said agreements.
	+ No user shall install unauthorized software such as but not limited to:
		- Non company managed licenses.
		- Pirated or otherwise illegally obtained software.
		- Demo or trial software without first obtaining permission from Information Management.
	+ Any software found in violation or deemed unauthorized by Information Management will be uninstalled.
* MOBILE DEVICES POLICY
	+ All mobile devices will be protected by a minimum of a four digit pin. Six digits are recommended if the device can be configured in such a manner.
	+ Lost or Stolen devices shall be reported immediately and the device will be remotely erased.
	+ All devices will have encryption activated to protect company data.
	+ Information Management is not responsible or accountable for backing up or restoration of personal information. Devices shall be reset and restored to company standards. Personally purchased applications will be the responsibility of the employee.

* REMOTE ACCESS POLICY
	+ Only authorized employees may connect to the network remotely. Such approvals will be generated by department manager.
	+ All external computers remotely accessing the network will have at a minimum:
		- Updated operating system, with recent critical patches installed.
		- Installed and updated anti-virus software.
		- Ability to encrypt via an installed client or web browsers.
	+ All activity while connected remotely comes under current policies including internet usage. Sessions will be logged.
* GUEST ACCESS POLICY
	+ Users requiring access to the internet will use a segregated public network which is not logically connected to any company resources.
	+ Guest use of company resources will require prior approval and will be given temporary user credentials and be subject to existing policies.
	+ All activity on public wireless is logged but not monitored.
	+ Guest access can be revoked without warning if any activity is deemed suspicious.
* MALWARE POLICY
	+ All company workstations will have updated anti-virus and malware protection installed. Updates will be managed by Information Management.
	+ Devices connecting remotely are required to have anti-virus installed.
	+ Employees shall not uninstall or disable anti-virus unless under the direction of Information Management.
	+ If a device has been detected as containing malware or a virus it will be denied access to network resources until such issues are resolved.
* CHANGE MANAGEMENT POLICY
	+ Account changes shall be generated by the department manager and forwarded to Information Management for processing. Any requests coming from accounts other than approved managers will not be reviewed.
	+ Access shall be granted using least privilege needed.
	+ Account change requests will be maintained in compliance with company policy.
	+ Random and routine audits of account and privilege requests will be performed by non-Information Management personnel on a bi-annual basis.
	+ User access may be changed without their notification if deemed needed by department management.