Acceptable Use of Technology Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

Policy Owner	Name the person/group responsible for this policy's management.
Policy Approver(s)	Name the person/group responsible for implementation approval of this policy.
Related Policies	Name other related enterprise policies both within or external to this manual.
Related Procedures	Name other related enterprise procedures both within or external to this manual.
Storage Location	Describe physical or digital location of copies of this policy.
Effective Date	List the date that this policy went into effect.
Next Review Date	List the date that this policy must undergo review and update.

Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy's basic objectives and what the policy is meant to achieve.

The purpose of this policy is to ensure that [Organization] systems and tools including computers, software, communication, network, and cloud-based tools, etc. provided to employees and contractors to enhance their productivity are used in a responsible way, ethically, and in compliance with all legislation and other [Organization] policies and contracts. This policy does not attempt to anticipate every situation that may arise and does not relieve anyone accessing any system of their obligation to exercise good judgment.

Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate "all" if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

This policy is applicable to all employees of [Organization], including full-time, part-time, and temporary employees; contractors; students; and interns. The requirements defined in this policy are applicable to all data, systems, and services owned and/or managed by [Organization].

Definitions

Define any key terms, acronyms, or concepts that will be used in the policy or accompanying procedures. A standard glossary approach is sufficient.

Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

Guidance	Section

Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy. Mapped regulations can be edited based on policy requirements.

#	Policy Statement	Mapped Regulations/Standards
1.	Acceptable use policies must be developed and communicated to stakeholders.	NIST CSF PR.AT-1 NIST 800-171 3.2.1 NIST 800-53 PL-4, PL-4(1) PS-6 SOC2SEC CC1.1, CC1.5 ISO 27001 7.2.2, 8.1.3, 12.2.1,13.2,18.1.2 PCI 12.3, 12.3.1, 12.3.2,12.3.3, 12.3.4, 12.3.5, 12.3.6, 12.3.7, 12.3.8, 12.3.9,12.3.10
2.	All devices and systems are property of [Organization] and all use must be in accordance with policies, standards, and guidelines.	
3.	[Organization] allows limited use of the network, systems, and devices for personal reasons (personal correspondences, online banking, etc.), but personal use must not be abused.	
4.	Personal use is acceptable, but it must not have a negative impact on overall employee productivity, cause additional expense to the company, compromise the company in any way, disrupt network performance, or contradict any other [Organization] policies in any way.	
5.	[Organization] assets and systems must not be used for illegal or unlawful purposes, including copyright infringement, obscenity, personal gain, libel, slander, fraud, defamation, plagiarism, intimidation, forgery, impersonation, illegal gambling, soliciting for pyramid schemes, and computer tampering (e.g. spreading computer viruses).	
6.	Users must not access and/or purchase technology, devices, applications, or services that are not formally authorized and approved by IT. (This circumvention of the IT department is known as Shadow IT.)	
7.	IT assets, such as laptops and mobile devices, must be used only by the people to whom they have been issued. The person to whom the device was issued is ultimately responsible for any actions performed with the device.	
8.	Users must always protect all corporate-managed IT assets, keeping them physically and logically secured and under the control of the user.	
9.	Access to [Organization] systems and devices must be controlled through individual accounts and passwords, as outlined in the password standard section of this document and in the Access Management Policy.	
10.	All voicemail boxes must be protected. Consider using a PIN (personal identification number). PINs must be changed every [insert period] to aid in mailbox security	
	Removable Media	
11.	Information should only be stored on removable media when absolutely required in the performance of the user's role (e.g. USB shared between two employees during a conference).	
12.	Mobile devices (e.g. smartphones, tablets) must not be used as removable media to transfer or store any business or customer data.	
13.	Any unknown removable media that is found unattended must be reported to the IT department and NOT inserted into any [Organization] issued device.	
14.	End users must take reasonable measures to secure removable media when not in use; not sharing with unauthorized users).	

15.	Use of removable media is not allowed on external or non-company-issued systems.
16.	Upon completion of the assigned duties, all data must be deleted from the removable media.
17.	All removable media must be turned in to the Service Desk for proper disposal when no longer required for business use.
	Electronic Communication and Internet Use
18.	Email systems and other messaging services used at [Organization] are owned by the company and are therefore its property and will be always monitored. Monitoring may include, but is not limited to, inadvertent reading by IT staff during the normal course of managing the email system, review by the HR and legal team during the email discovery phase of litigation, and observation by management in cases of suspected abuse or employee inefficiency.
19.	Employees of [Organization] with email accounts must check their email in a consistent and timely manner so that they are aware of important company communication, announcements, and updates as well as information for fulfilling business and role-oriented tasks.
20.	Electronic communication and internet must not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment (including offensive and/or insulting content), discrimination, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses).
21.	[Organization] communication platforms and internet must not be used for purposes that could be reasonably expected to strain storage or bandwidth (e.g. emailing large attachments instead of pointing to a location on a shared drive). Individual use of resources must not interfere with others' use of [Organization] email system and services.
22.	Users are prohibited from using accounts that do not belong to them and are prohibited from using platforms to impersonate others.
23.	Users must not give the impression that they are representing or providing opinions on behalf of [Organization] unless otherwise authorized.
24.	Users must not open message attachments or click on hyperlinks sent from unknown or unsigned sources through any platform (email, instant message, social media, etc.).
25.	[Organization] prohibits use of email or other messaging platforms for mass unsolicited mailings, chain letters, and competitive commercial activity unless preapproved by [Organization].
26.	Email users must be responsible for mailbox management, including organization and cleaning.
27.	Any allegations of misuse should be promptly reported to Service Desk. If you receive an offensive or suspicious email, do not forward, delete, or reply to the message. Instead, report it directly to Service Desk.
28.	Archival and backup copies of email messages must exist, despite end-user deletion, in compliance with [Organization]'s Records Retention Policy.
29.	Email access must be terminated when the employee or third party terminates their association with [Organization], unless other arrangements are made.
30.	[Organization] is under no obligation to store or forward the contents of an individual's email inbox/outbox after the term of their employment has ceased.
31.	Users must not send sensitive information that is not appropriately protected (encrypted).

32.	Users must take extra precautions when transmitting company, client, and/or other regulated information via electronic communications. Sensitive material must be marked and encrypted appropriately. Keep in mind that all email messages sent outside of [Organization] become the property of the receiver.
33.	Users must not automatically forward emails received by their [Organization] account to an external email address or other messaging system.
34.	[Organization] assumes no liability for direct and/or indirect damages arising from the user's use of [Organization]'s email system and services. Users are solely responsible for the content they disseminate. [Organization] is not responsible for any third-party claim, demand, or damage arising out of use of [Organization]'s email systems or services.
35.	[Organization] may monitor any/all internet activity originating from company-owned equipment or accounts or taking place over company networks.
36.	Users are permitted to remotely access the corporate network while offsite. Users must use the approved VPN service(s). Users will be required to authenticate using multifactor authentication (MFA). Only authorized users are permitted to access the network through VPN.
	Social Media
37.	[Organization] social media accounts must be used for business purposes only. These purposes include building positive brand image, providing customer support, monitoring public opinion, professional networking, and more as approved.
38.	Access to social media must be open to staff who have received approval from their manager. Approval will be provided given a legitimate business purpose.
39.	All actions and communications through social media must adhere to all previously defined acceptable use of electronic communications. Staff representing [Organization] on social media must [participate in mandatory training, sign an agreement, or other].
40.	The use of personal social media accounts and user IDs for company use is prohibited.
41.	The use of [Organization] social media user IDs for personal use is prohibited.
	Data Security
42.	All organizational data is owned by [Organization] and, as such, all users are responsible for appropriately respecting and protecting all data assets.
43.	Users must not view, copy, alter, or destroy data, software, documentation, or data communications belonging to [Organization] or another individual without authorized permission.
44.	Users must keep all data secure by taking precautions and following requirements defined in this policy, [Data Classification Policy], and the data-handling requirements defined in the [Data Classification Standard].
45.	Data must be classified based on sensitivity. Data must be classified as ["top secret," "confidential," "internal," "limited," or "public"]. Data at each classification level must be safeguarded and handled appropriately in accordance with the [Data Classification Standard].
46.	Users must only access data provided to them for duties in connection with their employment or engagement and in accordance with their terms and conditions of employment or equivalent.
47.	Extraction, manipulation, and reporting of [Organization] data must be done for business purposes only.

48.	Personal use of organizational data, including derived data, in any format and at any location, is prohibited.
49.	Users must follow all company-sanctioned data removal procedures to permanently erase data from devices once its use is no longer required, as defined in the [Data Classification Standard]. Data must be retained for the length of time defined in the [Data Retention Policy].
	Mobile Device Use
50.	It is the responsibility of any employee of [Organization] who uses a mobile device to access corporate resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. Any mobile device that is used to conduct [Organization] business must be used appropriately, responsibly, and ethically.
51.	IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to corporate and corporate-connected infrastructure.
52.	All mobile devices used to access company systems and/or data (such as email) must be protected by a strong access control (e.g. alphanumeric password or biometric authentication). Employees must not disclose their passwords to anyone.
53.	All users of mobile devices must employ reasonable physical security measures.
54.	Any non-corporate computers used to synchronize or back up data on mobile devices must have up-to-date antivirus and anti-malware software.
55.	Sensitive data (e.g. client data) and passwords must not be stored on mobile devices.
56.	In the event of a lost or stolen mobile device that has access to [Organization] resources (e.g. email, OneDrive, Authenticator), the user must report the incident to Service Desk immediately.
57.	All personal mobile devices attempting to connect to the corporate network through the internet must be inspected using technology centrally managed by the [Organization] IT department. Devices that are not approved by IT, are not in compliance with IT's security policies, or represent any threat to the corporate network or data will not be allowed to connect.
	Clean Desk and Printing
58.	Employees must ensure that all sensitive information in hardcopy or electronic form is always secure in their work area.
59.	Computer workstations must be locked (screen/keyboard) when workspace is unoccupied.
60.	Laptops must be either locked with a locking cable or locked away in a drawer if not taken home at the end of the workday.
61.	Any sensitive information (e.g. client data) must be removed from the desk and locked away when the desk is unoccupied.
62.	Passwords must not be written down anywhere under any circumstances.
63.	File cabinets containing sensitive information must be kept closed and locked when not in use or when not attended.
64.	Keys/badges used for access to sensitive information must not be left at an unattended desk.
65.	Printouts containing sensitive information must be immediately removed from the printer.
66.	Upon disposal, sensitive documents must be shredded.
67.	Whiteboards containing sensitive information must be erased.

	Passwords
68.	Access to [Organization] systems and devices must be controlled through individual accounts and passwords.
69.	Users must not share account or password information with another person. Accounts are to be used only by the assigned user of the account and only for authorized purposes.
70.	A user must contact the Service Desk to obtain a password reset if they have reason to believe any unauthorized person has obtained their password.
71.	Users must not use corporate passwords for other services. In the event that other services are compromised, it could leave corporate accounts compromised as well.
72.	Password complexity must be enforced by IT through system-enforced policies to ensure strong passwords and proper password hygiene.
	Incident Response and Reporting
73.	[Organization] must have an incident response program for efficient remediation of information security incidents.
74.	Users must report any suspected security incident to the Service Desk.
75.	Users must cooperate with incident response processes, such as forfeiting their equipment to Service Desk for investigation if it is potentially compromised.
	Security Awareness and Training
76.	During onboarding, all users must undergo information security awareness and training. Upon completion, users must be required to sign a declaration that they have completed training, understand the requirements and specific procedures taught, and intend to abide by the policies and procedures provided.
77.	Users must complete ongoing security awareness and training as scheduled by the [IT Department].
	Security Unacceptable Use
78.	Users must not introduce malicious programs into the network or a system (e.g. viruses, worms, Trojan horses, email bombs).
79.	Users must not introduce or contribute to security breaches or disruptions of network communication.
80.	Port scanning or security scanning is expressly prohibited unless prior approval is granted.
81.	Users must not execute any form of network monitoring that will intercept data not intended for the employee's host unless this activity is approved as part of the employee's normal job/duty.
82.	Users must not circumvent user authentication or security of any host, network, or account.
83.	No servers (i.e. running web or FTP services from user workstations) or devices that actively listen for network traffic must be put on the corporate network without approval.
84.	Users must not interfere with or deny service to any other user (for example, denial of service attack).

Relevant Procedures

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is a best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies.
2. Termination of employment.
3. Legal action according to applicable laws and contractual agreements.

Agreement

Include a section that confirms understanding and agreement to comply with the policy. Both signatures and dates are required. A sample statement is provided below.

I have read and understand the [name of policy]. I understand that if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or company policy.

_____
Employee Name

_____ _____
Employee Signature Date

Revision History

Version ID	Date of Change	Author	Rationale