Acceptable Use Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

Information systems are a growing and important resource for ABC Company Staff, one that can provide critical competitive advantage to ABC Company in the form of information gathering, improved external communications, and increased customer responsiveness. As more and more of our Staff use Information Systems to connect with our customers, suppliers and other key organizations, it is important that ABC Company Staff understand and agree on the appropriate procedures to protect ABC Company’s assets.

# II. Purpose

This policy provides useful tips and techniques to promote effective use of ABC Company’s Information Systems. It applies to all ABC Company systems located on or accessed from ABC Company property and systems provided by ABC Company for use in ABC Company business.

# III. Scope

This policy applies to all ABC Company Staff that have access to ABC Company’s Information Resources.

# IV. Policy

ABC Company utilizes sophisticated computer and communications systems to assist Staff in performing their job functions. These technologies support our business activities by enabling closer, more effective and timely communications among personnel within the ABC Company and with our customers, partners and vendors worldwide. These guidelines advise all users regarding the access to and the disclosure of Information Systems. These guidelines establish the ABC Company's expectations for all Staff concerning the disclosure of information via ABC Company’s Information Systems.

ABC Company maintains and uses many facilities, equipment, and communication systems, such as telephones, regular mail, special delivery services, E-mail, voice mail, fax machines, computers, etc., designed to make the ABC Company’s operations effective and efficient. ABC Company’s Information Systems are provided to Staff at ABC Company expense to assist Staff in carrying out ABC Company business. Some of these systems permit Staff to communicate with each other internally and with other parties externally. As with all ABC Company assets, ABC Company’s Information Systems are for official ABC Company business only. Access to ABC Company Information Systems is provided in conjunction with the official ABC Company business and individual job responsibilities. Use of ABC Company’s Information Systems is subject to these policies and guidelines and other relevant ABC Company policies and procedures.

A. Information Access, Content, and Use

The ABC Company makes every effort to provide its Staff with the best technology available to conduct the ABC Company's official business. The ABC Company has installed, at substantial expense, Information Resources to conduct its official business.

This document addresses general Information Systems policies and guidelines, specific issues related to appropriate content, and Staff use of ABC Company’s Information Systems. All departments and Staff are required to follow these general policies and guidelines. All ABC Company Staff with access to ABC Company’s Information Systems are required to read, understand and comply with ABC Company's policies.

ABC Company’s Information Systems are owned by ABC Company and are to be used for business purposes only in serving the interests of ABC Company’s customers and in the course of normal business operations.

The use of ABC Company facilities, property, equipment, or communication systems is limited to Acceptable Use as defined in these policies and guidelines. No ABC Company equipment or communications systems, including all hardware and software, may be removed from ABC Company property without prior express consent of the ABC Company.

Personal equipment, including all computer hardware and software, may not be brought onto ABC Company premises or be used for ABC Company’s official business without the prior express consent of the ABC Company. Staff are not to use their personal accounts during work hours or use ABC Company equipment to reach personal sites unless it is for legitimate business purposes, as determined solely by ABC Company.

The ABC Company encourages the use of ABC Company’s Information Systems for business when such business can be accomplished consistent with the following policies and guidelines identified in this document. When using Information Systems, Staff shall conduct official ABC Company business consistent with the ABC Company's mission statement. Official ABC Company business shall comply with all federal and state statutory requirements as well as standards for integrity, accountability, and legal sufficiency. Thus, official ABC Company business conducted via the Internet should meet or exceed the standards of performance for traditional methods (e.g. meetings, use of telephone).

Staff shall base decisions to use ABC Company’s Information Systems on sound business practices. The conduct of business using ABC Company’s Information Systems is particularly compelling where costs are reduced and/or the services provided by the ABC Company are improved in measurable ways. When using ABC Company’s Information Systems, ABC Company Staff shall promote and maintain a professional image.

ABC Company Staff shall disseminate information that is current, accurate, complete, and consistent with ABC Company policy. Information released via ABC Company’s Information Systems is subject to the same official ABC Company policies for the release of information via other media (such as printed documents), so that the information disclosed avoids potential problems with copyrights, trademarks, and trade secrets. Information accuracy is particularly important.

ABC Company Staff shall protect confidential and proprietary information entrusted to the ABC Company. Questions regarding confidential or proprietary information should be directed to ABC Company management or his/her designee.

B. Protecting Confidential Information

Maintaining the confidentiality of sensitive information is crucial to ABC Company's success. Confidential information stored on or carried over ABC Company’s Information Systems could become the subject of accidental or intentional interception, mis-delivery, hacking or even unauthorized internal review unless Staff take the necessary precautions outlined in these guidelines.

ABC Company has developed specific procedures to ensure the protection of confidential information. Staff should exercise care when communicating any potentially confidential information outside of ABC Company, as no electronic communications facility is completely secure.

Data shall be classified per the Data Classification Policy. All confidential data should be marked with "Confidential," "Do not reproduce," "Not to be reproduced without approval," or "Do not forward." All E-mail messages containing confidential information should contain "Confidential" in the subject header.

Some directories in the ABC Company’s Information Systems contain sensitive or confidential data. Access to these directories shall be restricted. Unauthorized attempts to circumvent such access restrictions are violations of these Guidelines and may result in disciplinary action, up to and including termination of employment, and legal action.

Staff must refrain from entering into discussions with third parties regarding the ABC Company's business prospects or financial condition. Staff should not discuss future products, services, features or functionality unless ABC Company has previously disclosed such information in a press release or through some other public disclosure. Such information is proprietary to ABC Company and constitutes valuable information that should be protected as a trade secret. The release of such information could become the subject of criminal prosecution.

Staff are asked to respect the privacy of individuals who send them messages. Staff should protect voice mail, and E-mail accounts from unauthorized access. Appropriate protection procedures include ensuring proper password protection to these accounts, closing E-mail messages after reading them and deleting all messages when they are no longer needed.

Staff shall not place ABC Company material (e.g. copyrighted software, internal correspondence) on any publicly accessible Internet computer without prior permission.

The Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet may be at risk of detection by a third-party. Staff must exercise caution and care when transferring such material in any form.

C. Copyrighted Information

ABC Company respects the intellectual property rights of other companies and individuals. Use of all copyrighted material, including literature, software, and graphics shall comply with relevant, valid license terms. ABC Company’s Information Systems may provide access to materials protected by copyright, trademark, patent and trade secret and even export laws. Staff should not assume that merely because information is available on an electronic information system such as the Internet, that it may be downloaded or further disseminated. No copyrighted material should be copied, transmitted, posted, or otherwise distributed without such compliance. If a question arises as to the propriety of downloading information, ABC Company management should be consulted.

All material trademarked or copyrighted by ABC Company should be marked with the appropriate trademark or copyright designation. No ABC Company Staff should remove trademark and copyright notices from third party material.

ABC Company’s license to use software is carefully set forth in legal agreements that ABC Company has with the developers and distributors of the software. Staff’s use of software must be in compliance with those agreements. If ABC Company gives Staff the opportunity to use certain software, copying of that software is strictly prohibited. Loading of software of a personal interest is prohibited unless Staff are given prior express consent by ABC Company management. When Staff leave ABC Company, all ABC Company owned software, licenses, and media will remain with ABC Company.

Unless otherwise noted, all software on the Internet should be considered copyrighted work. Therefore, Staff members are prohibited from downloading software and/or modifying any such files without permission from the copyright holder.

D. Privacy Statement

This policy is intended to guide Staff in the performance of their duties. It is also intended to place Staff on notice that Staff should not expect ABC Company’s Information Systems and their contents, to be confidential or private. All data, including any that is stored or printed as a document, is subject to audit and review.

No Staff member has a reasonable expectation of personal privacy with respect to the use of any of the ABC Company’s facilities, property, equipment or communications systems. This includes anything created or received on ABC Company’s Information Systems even if used for business purposes and in the normal course of ABC Company operations.

ABC Company reserves the right, but not the obligation, to monitor use of ABC Company’s Information Systems including the Internet, E-mail, computer transmissions, and electronically stored information created or received by ABC Company Staff with the ABC Company's Information Systems. All computer applications, programs, work-related information created or stored by Staff on ABC Company's Information Systems, are ABC Company property.

E. Monitoring and Inspecting Information Systems

ABC Company’s Information Systems are provided for official ABC Company business. ABC Company’s Information Systems are owned and controlled by the ABC Company and are accessible at all times by the ABC Company for maintenance, upgrades and other business or legal purposes.

All Information Systems, including the messages and data stored on the systems, are and remain at all times the property of ABC Company, subject to applicable third party intellectual property rights such as copyrights. By virtue of continued employment and use of ABC Company systems, all Staff are considered to have consented to monitoring and other access by authorized ABC Company personnel. ABC Company reserves the right to inspect a Staff member’s computer system for violations of ABC Company policies.

ABC Company reserves the right to access and conduct an inspection or search all directories, indices, files, databases, faxes, ABC Company computer hardware and software, voice mail, E-mail and communication systems or deliveries sent to any ABC Company location, and other Information Resources no matter to whom it is addressed, with no prior notice. ABC Company may also cancel or restrict any Staff’s privilege to use any or all of its facilities, equipment, property, or communication systems.

If a Staff member refuses to cooperate with a search or inspection for legitimate business purposes that is based on reasonable suspicion that the Staff is in possession of prohibited materials, ABC Company may take that refusal into consideration in determining appropriate disciplinary action. A Staff member’s refusal to provide their password to ABC Company management will be considered additional grounds for discipline. Discipline, including termination, will be based on all available information, including the information giving rise to the inspection or search.

Access to on-line services, the Internet, blogs, social media sites, or other communications networks is prohibited unless ABC Company has provided prior express consent. As such, no ABC Company equipment, telephone lines, or on-line services may be used to view or download offensive, discriminatory or pornographic material. Employee use of these services may be monitored to include numbers called and the amount of time spent using the services. ABC Company reserves the right to inspect computer systems for viruses, offensive, discriminatory or pornographic material, personal software, etc.

ABC Company management may examine Staff communications or files and such examination should be expected to occur in various circumstances when necessary, including, but not limited to:

* Ensuring that ABC Company systems are not being used to transmit discriminatory, harassing or offensive messages of any kind.
* Determining the presence of illegal material or unlicensed software.
* Ensuring that communication tools are not being used for unauthorized, disruptive, or improper uses.
* Investigating allegations or indications of impropriety.
* Locating, accessing and/or retrieving information in Staff absence.
* Responding to legal proceedings and court orders in the preservation or production of evidence.
* ABC Company reserves the right to review Staff use of and to inspect all material created by or stored on ABC Company Information Systems. ABC Company reserves the right to monitor all use of Information Systems to access, review, copy, delete, or disclose messages and data derived from any use. All messages or data become property of ABC Company, subject to access, review, duplication, deletion, or disclosure by ABC Company management or by other personnel authorized by ABC Company. Staff should be aware that billing practices, firewall protections, and traffic flow monitoring programs often maintain detailed audit logs setting forth addresses, times, durations, etc. of communications both within and external to the ABC Company. Staff should treat ABC Company’s Information Systems with the expectation that communications will be available for review by authorized personnel of ABC Company for legitimate business purposes at any time.

ABC Company reserves the right to access, review, duplicate, delete or disclose for legitimate business purposes any communications, messages or data derived from use of ABC Company's Information Systems.

F. Storing and Archiving Information

ABC Company has developed specific archival procedures to ensure the safe retention of electronic data. Most files are subject to routine back-up procedures. Copies of documents and electronic messages may be retained for long periods of time. By virtue of various archival practices employed at ABC Company, any messages or data stored, even temporarily, on ABC Company Information Systems may be copied to magnetic or other storage media without the specific knowledge of the individual creating the messages or data. Such archives are and remain ABC Company property and may be used by the ABC Company for any business purpose. Simply deleting messages or data from these Information Systems does not provide privacy with regard to such messages or data. The length of time that such archives may be maintained can be almost indefinite. Staff may be required to preserve their electronic data based on pending litigation and/or investigations by the ABC Company. Refer to the Data Retention Policy for more information on storing and archiving information.

G. Employee Usage

Each Staff has the responsibility of complying with ABC Company’s policies and guidelines provided in this document. Failure to do so may result in disciplinary action, up to and including termination of employment and legal action.

The use of Information Systems is restricted to official ABC Company business. Personal use of or time spent for personal gain is strictly prohibited unless ABC Company gives prior express consent. Inappropriate personal use includes the creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials, materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited. In addition, any Internet use that could cause congestion, disruption of normal service, or general additional ABC Company expense is prohibited.

Hacking or unauthorized attempts or entry into any other computer is forbidden. Such an action is a violation of the Federal Electronic Communications Privacy Act (ECPA) 18 U.S.C. 2510.

Sending threatening, slanderous, racially and/or sexually harassing messages is strictly prohibited. The representation of yourself as someone else, real or fictional, or a message sent anonymously is prohibited.

Staff should be aware that ABC Company’s Information Systems and the World Wide Web are not censored and contain information some users may find offensive. ABC Company cannot accept responsibility for what the Staff accesses. However, if offensive material is accessed, Staff shall disengage from the material immediately.

Staff shall not copy or transfer electronic files without prior ABC Company permission. Almost all software is subject to Federal copyright laws. Care should be exercised whenever accessing or copying any information that does not belong to the Staff. When in doubt, consult ABC Company management. Unauthorized or illegal use of third-party intellectual property is prohibited. Such use includes, but is not limited to, downloading or using copyrighted or patented software, video and audio clips or documents on ABC Company’s Information Systems in a manner inconsistent with relevant license terms or other intellectual property rights.

Downloading a file from the Internet can infect ABC Company’s systems with a virus. Staff shall not circumvent or disable ABC Company standard virus prevention software and/or Information Resource security mechanisms.

Staff shall not send post or provide access to any confidential ABC Company materials or information to anyone outside of ABC Company.

Staff are obligated to cooperate with any investigation regarding the use of Staff computer equipment and which ABC Company management has authorized.

Alternate Internet Service Provider connections to ABC Company’s internal network are not permitted unless prior express consent has been given by ABC Company management and properly protected by a firewall or other appropriate security device(s).

If Staff are using information from an Internet site for strategic official ABC Company business decisions, Staff should verify the integrity of that information. Staff should verify whether the site is updated on a regular basis (the lack of revision date might indicate out-of-date information) and that it is a valid provider of the information.

ABC Company has no control or responsibility for content on an external server not under the control of the ABC Company. Information may be offensive and/or unsuitable for dissemination.

Do not upload or download large files during prime hours due to the network impact on other users. Information Systems may have limits regarding disk space usage. Documents take up space; therefore, Staff should regularly delete and/or archive any files Staff wish to save.

Staff using ABC Company’s accounts are acting as representatives of the ABC Company. As such, Staff should act accordingly so as not to damage the reputation of ABC Company.

H. Information Systems Awareness

The use of Information Systems is the responsibility of each Staff. The practices listed below are not inclusive, but rather designed to remind each Staff of the need to raise their Information Systems awareness.

* Protect equipment. Keep it in a secure environment and keep food and drink from electronic systems. Know where the fire suppression equipment is located and how to use it in an emergency.
* Protect areas. Keep unauthorized people away from equipment and data. Challenge strangers in the area
* Protect passwords. Never write it down or give it to anyone. Don't use names, numbers or dates that are personally identified with the Staff. Change the password often and change it immediately if it has been compromised.
* Protect files. Don't allow unauthorized access to Staff files and data. Never leave equipment unattended with the password activated – log off.
* Backing up data. Keep duplicates of critical data in a safe place.
* Report security violations. Staff should tell their supervisor or ABC Company management if Staff see any unauthorized changes to Staff data. Immediately report any loss of data or programs, whether automated or hard copy.

I. Electronic Mail (E-mail) and Etiquette

E-mail may be sent through each Staff's computer. E-mail will be sent for official ABC Company business only. No personal E-mail shall be sent or received via ABC Company Internet accounts.

ABC Company Staff should not attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading. Management reserves the right, but not the obligation, to access all E-mail files created, received or stored on ABC Company-funded systems and such files can be accessed without prior notification.

ABC Company Staff are expected to maintain their E-mail accounts on a regular basis. This entails deleting E-mail once it has been read or sent. Excess E-mail takes up unnecessary storage space on the server and may cause the entire system to run slowly.

E-mail requires extensive network capacity. Sending unnecessary E-mail, or not exercising constraint when sending very large files, or sending to a large number of recipients consumes network resources that are needed for critical official ABC Company business. When ABC Company grants an individual Staff access to the network, it is the responsibility of Staff to be cognizant and respectful of network resources.

E-mail users are to exercise good judgment and common sense when creating and distributing messages. E-mail is the property of the ABC Company and is to be used exclusively for official ABC Company business. No Staff E-mail is considered private. Similarly, the accessing, reading or copying of E-mail not intended for a Staff member’s eyes is prohibited. Staff are strictly prohibited from sending E-mail messages of a harassing, intimidating, offensive or discriminatory nature. Anonymous messages are not to be sent. Staff are prohibited from using aliases while connected to services. ABC Company retains the right to access a Staff member's E-mail at any time for any reason without notice to the Staff. Conduct in violation of this policy will subject Staff to ABC Company’s disciplinary procedures.

Mail on the internet is not secure. Never include in an E-mail message anything private and confidential. E-mail is sent unencrypted and is easily read. If anything but plain text is sent as an E-mail, be careful. Recipients may not have the ability to translate other documents, for example Word or Excel documents.

State the subject of the message in the subject line.

Include a signature (an identifier that automatically appends to the E-mail message) that contains the method(s) by which others can contact Staff (usually Staff’s E-mail address, phone number, faxes number, etc.).

For important items, let senders know Staff has received their E-mail, even if Staff cannot respond in depth immediately. They need to know their E-mail is not lost.

Watch punctuation and spelling. It can reflect on Staff’s professionalism. Use automatic spell checking programs if available.

Be careful when sending replies - make sure Staff is sending to a group when intent is to send to a group and to an individual when Staff intent is to send to an individual. It is best to address directly to a sender(s). Check carefully, the "To" and "From" before sending mail. It can prevent unintentional errors.

Never send angry messages (flames). If Staff receives a "flame", do not over react. Remember that not everyone is polite. DO NOT SEND MESSAGES ALL IN CAPITALS. It looks like shouting. Use initial capitals or some other symbol for emphasis. For example: That IS what I meant. That \*is\* what I meant.

Remember that some people have to pay for each byte of data they receive. Please keep messages to the point without appearing terse or rude.

The use of Information Systems should be consistent with ABC Company's core values when communicating with both Staff and external parties. Particularly, the values of honesty, integrity and mutual respect should govern Staff’s use of Information Systems. When using voice mail and E-mail systems for communicating with other individuals over Information Systems, Staff should consider the following principles:

* Be courteous - Refrain from saying anything electronically that you would not say to the recipient face-to-face.
* Keep messages brief - Include only one topic per message, and start the main point in the first sentence.
* Proofread messages - E-mail messages drafted in haste can be difficult to follow and easy to misinterpret. Do not ignore the basics of writing in E-mail correspondence.
* Use a descriptive subject line - When using E-mail, never leave a subject line blank. Remember to use brief but informative message headers.
* Properly prioritize - Do not overstate the urgency of the message simply to get attention. "Urgent" designations should be limited to messages that require immediate response from the recipient.
* Send messages only to appropriate individuals - Send E-mail on a need-to-know basis only. Unnecessary messaging should be avoided as it decreases the effectiveness of ABC Company systems.
* Identify the message sender - No E-mail or other electronic communication may be sent which attempts to hide the identity of the sender, or represent the sender as someone else or from another organization.
* Use attachments wisely - Some individuals have systems that cannot read attachments in E-mail messages. Staff using UNIX workstations may not be able to read attached Word documents. Voice mail attachments may contain irrelevant information.
* Respond with care - Be careful not to use "Reply all" unless you intend all other recipients to receive your response.
* Think before forwarding messages - Think of the sender's intentions before forwarding private communications.

J. Securing Information Systems With Passwords

Prior express consent for Information Systems access must be obtained through ABC Company management. Staff of contractors shall only be given access to the network after written communication and approval by ABC Company management. Once ABC Company provides prior express consent, Staff shall be responsible for the security of their account password and will be held responsible for all use or misuse of his or her account. No other password or security device shall be used without approval by ABC Company management.

Each ABC Company Information System may allow Staff to set or change their password. If so, set the password and change it regularly. Guidelines for choosing and setting passwords should be obtained from the Password Policy. Periodic password changes keep undetected intruders from continuously using the password of a legitimate user. After logging on, the computer will attribute all activity to a Staff member’s user id. Therefore, never leave workstations without logging off -- even for a few minutes. Always log off or otherwise inactivate the workstation so no one could perform any activity under Staff’s user id when away from the area. Staff should safeguard sensitive information from disclosure to others.

If requested, Staff shall disclose their passwords (e.g. voice mail, E-mail, relevant Internet web site passwords) to their supervisor and/or manager. Staff must maintain secure passwords and never use an account assigned to another user.

ABC Company reserves the right to override the user's password and other security features when it has a need to do so. Should a time come when Staff leaves the ABC Company, or at any other appropriate time, the ABC Company may replace Staff’s password with another of the ABC Company’s choosing.

K. Protecting Information Systems

ABC Company provides virus protection software to help safeguard Information Systems. These systems are not totally foolproof. As such, be particularly cautious when opening any E-mail with an attachment.

Staff shall not disable or remove anti-virus software. Viruses can infect executable files, disk boot sectors, documents, etc. If a virus is received from a sender, that sender should be notified that the file was infected and, if possible, the type of virus should be identified.

Network administrators shall ensure that only fully supported web browsers and e-mail clients are allowed to execute in the organization, ideally only using the latest version of the browsers and e-mail clients provided by the vendor.

Network administrators shall use Domain Name System (DNS) filtering services to help block access to known malicious domains. To lower the chance of spoofed or modified e-mails from valid domains, network administrators shall implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.

L. Encrypting Data

Only authorized encryption tools (both software and hardware) may be used in connection with Information Systems. Except with the prior written consent of ABC Company management, all encryption tools must permit the ABC Company to access and recover all encrypted information.

M. Securing Mobile Computing Devices

Staff who use ABC Company mobile computing resources (laptops, hand held devices, etc.) must take adequate precautions to ensure that proprietary information contained in such devices is secure and not available to third parties, particularly during travel. Staff are responsible for taking adequate precautions against theft of their mobile computing devices. Please refer to the Bring Your Own Device and Technology Policy for more information.

N. Acceptable Use

* Authorized Use. The authorized use of ABC Company systems is limited to ABC Company’s official business. The ABC Company provides Information Systems and communication tools to facilitate business communication and enhance personal productivity. ABC Company reserves the right to prohibit or restrict use of ABC Company systems for any other purpose and at any time.
* Incidental Personal Use. Personal use of ABC Company systems is permitted so long as it is not excessive as determined by the ABC Company, does not interfere with job performance, consume significant resources, or interfere with the activities of other Staff.

O. Unacceptable Use

* Unauthorized Use. Excessive personal and other use of Information Systems inconsistent with this or any other ABC Company policy is unauthorized. Under no circumstances are ABC Company’s Information Systems to be used for personal financial gain or to solicit others for activities unrelated to official ABC Company business, such as solicitations for personal, political, or religious causes. Installation of software without approval from ABC Company management is unauthorized.
* Disruptive Use. Use that may reasonably be considered offensive or disruptive to any individual or organization, or to harmony within the workplace is prohibited. Such disruptive use includes, but is not limited to, transmission, retrieval, storage, or display of defamatory, obscene, offensive, politically motivated, slanderous, harassing, or illegal data, or messages that disclose personal information without authorization. Grossly indiscriminate or "broad band" distribution of E-mail would clearly constitute a disruptive use.
* Prohibited use. Unauthorized or illegal use of third-party intellectual property is prohibited. Such use includes, but is not limited to, downloading or using copyrighted or patented software, video and audio clips or documents on Information Systems in a manner inconsistent with relevant license terms or other intellectual property rights. When in doubt about the existence or scope of a license or about appropriate use of copyrighted, patented, or otherwise proprietary third-party data or software code, Staff should contact ABC Company management. Staff are expressly prohibited from using ABC Company’s Information Systems to store or access pornography.

Only the IT Department is authorized to install software on servers, storage, and other related Information Resources.

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff who use Information Resources.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT APO01.02, APO01.11, APO07.03, APO07.05, APO13.01, APO13.02, DSS04.05

GDPR Article 32

HIPAA 164.308(a)(1)(ii)(B), 164.312(a)(2)(iv)

ISO 27001 7.3, A.7.2, A.8.1.3, A.8.2

NIST SP 800-37 3.3

NIST SP 800-53 3.2, 3.4, 3.16

NIST Cybersecurity Framework ID.AM-6, ID.GV-2, DE.DP-2

PCI 12.3.5