Data Privacy 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

ABC Company’s computer systems and related devices collect and record activity for business purposes. This information should not be disclosed to unauthorized individuals.

# II. Purpose

This policy establishes general privacy requirements for information automatically generated by computer systems and network devices, including systems and devices involved in the transmission and storage of voice data. The policy further delimits the conditions under which network data may be disclosed.

# III. Scope

This policy applies to all ABC Company Staff who use Information Resources.

# IV. Policy

A. Network Data

In the course of normal network operations, computer systems, voice systems, access control systems, and network devices may automatically generate and track logging data, source and destination internet protocol (IP) addresses, session times, port numbers, file sizes, etc. (Network Data).

It is the general policy of ABC Company to treat Network Data as private. This information may be obtained, stored, and reported for legitimate business purposes but shall not be exposed to unauthorized individuals except as specifically listed below.

B. Exceptions

Network Data may be exposed or disclosed under the circumstances listed below.

To maintain the integrity and availability of network operations. Network Data may intentionally or inadvertently expose Information Resources stored on networked machines or transmitted through the network in the following situations:

* Network performance monitoring or troubleshooting.
* Moving data through the network via automated store-and-forward systems.
* Copying, archiving, or otherwise preserving portions of messages transmitted over the network in the course of routine network maintenance activities.

In the event that messages or data files within the network indicate the presence of activities that violate internal policies or law.

In the event of recognized network security threats. ABC Company reserves the right to investigate and remediate possible network security threats, including by means of capture, logging, and examination of files, communications, and other traffic and transmissions over or on the network.

In response to a court order.

In the event of a legitimate health or safety emergency.

In pursuit of reasonable business interests, such as fulfillment of partnership agreements.

C. Requests for Network Data

All requests to retrieve and share Network Data must be submitted to the IT Department and must be approved by the appropriate Department head. Such requests shall include:

* Name and role of the requestor.
* Reason for the request, in accordance with the principles set forth in this policy.
* Intended use of the requested data.

Any network data intentionally shared with third parties must be sanitized to preserve the anonymity of network users.

# 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.

**Policy History**

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

**References:**

COBIT EDM01.01, EDM03.02, APO01.11, APO13.07, APO14.01-02, APO14.07, APO14.10

GDPR Article 32

HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E)

ISO 27001 A.8.2

NIST SP 800-37 P-10

NIST SP 800-53 PM-29, RA-2

NIST Cybersecurity Framework ID.AM-5, ID.GV-3, ID.RM-1, DE.DP-2

PCI 3.1, 12.2