TERMS AND DEFINITIONS 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 has established a common set of terms and definitions for all policies, procedures, plans, and related documents.

# II. Purpose

With consistent terms and definitions, ABC Company Staff increase uniformity and understanding while reducing confusion and errors.

# III. Scope

The following terms and definitions apply to all ABC Company communications, policies, procedures, plans, and related documents.

# IV. Policy

ABC Company provides the following list of terms and definitions:

Bring Your Own Device (BYOD) – Staff owned equipment including laptops, notebooks, smartphones, tablets, and related devices.

Bring Your Own Device and Technology (BYODT) – includes both BYOD and BYOT.

Bring Your Own Technology (BYOT) – Staff owned operating systems, software applications, browsers, tools, utilities, scripts, software development kits, cloud services, and related technologies.

Certificate Authorities (CA) – sign and distribute certificates used to assure an identity when establishing encrypted communications.

Chief Security Officer (CSO) – person responsible for information security, physical security, and security of Information Resources.

Classified Information – information that Executive Order 13526, ‘‘Classified National Security Information,’’ December 29, 2009 (3 CFR, 2010 Comp., p. 298), or the Atomic Energy Act of 1954, as amended, requires to have classified markings and protection against unauthorized disclosure.

Cloud Computing – the use of computing resources (e.g. hardware and software) that are delivered as a service over a network (typically the Internet).

Controlled Unclassified Information (CUI) – information (excluding Classified Information) that requires safeguarding or dissemination controls required by laws, regulations, or Government-wide policies.

Data Owner – the principal user/manager of an application or Information System.

DMZ (demilitarized zone) – a computer host or small network inserted as a "neutral zone" between a private network and an outside public network (e.g. Internet). It prevents outside users from gaining direct access to a server that has company data.

Executive Management – ABC Company President and Vice Presidents.

Information Resources – facilities, hardware, software, Staff, and related resources.

Internet Protocol (IP) – communications protocol for routing packets across network boundaries (e.g. the Internet).

Information System – information collected, transmitted, stored, and/or archived using telephones, cell phones, pagers, voice mail, electronic mail accounts (E-mail), Internet, the World Wide Web (WWW), LAN/WAN access software, ABC Company intranet, computers, servers, networks, peripherals, fax machines, modems, firewalls, routers, switches, hubs, and related equipment.

Information Technology (IT) – the use of computers and telecommunications equipment to store, retrieve, transmit and manipulate data.

Intranet – internal LAN used by authorized ABC Company Staff.

LAN – Local Area Network.

Malware – malicious software including viruses, spyware, Trojan Horse programs, worms, and similar types of programs.

Personal Information – includes the following:

* Audio, electronic, visual, thermal, olfactory or similar information.
* Biometric information.
* Characteristics of protected classifications under state or federal law.
* Commercial information including records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies.
* Education information, defined as information that is not publicly available personally identifiable information (PII) as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
* Geolocation data.
* Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier IP address, e-mail address, account name, Social Security number, driver’s license number, passport number, or other similar identifiers.
* Inferences drawn from any of the information identified in this definition to create a profile about an individual reflecting the individual’s preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.
* Internet or other electronic network activity information including, but not limited to, browsing history, search history and information regarding a consumer’s interaction with a website, application or advertisement.
* Professional or employment-related information.

Mobile Computing Device – includes laptops, notebooks, netbooks, tablets, and similar devices.

Removable Media – portable media including CDs, DVDs, memory sticks, flash drives, USB drives, portable hard drives, backup tapes, and related media.

Resource Owner – individual assigned the responsibility of granting, changing, and terminating access to an asset. Makes important decisions regarding the resource or asset.

Security Policy - the term “security policy” has several meanings. Policy can refer to ABC Company management’s directives to create an information system security program, establish its goals, and assign responsibilities. Policy can also refer to the specific security rules for particular systems. Policy may refer to specific managerial decisions such as e-mail privacy policy or password policy. Since policy may be developed and written at a broad level, all three types of policy must be supplemented with additional procedures, plans, and guidelines.

Sensitive Information – privileged or proprietary information which, if compromised through unauthorized disclosure, alteration, corruption, loss, or misuse could cause serious harm to ABC Company.

Smartphone – a mobile phone that allows advanced computing and communications activity.

Staff – ABC Company employees and other resources including contractors, vendors, and third-party business partners.

Tenant – a customer who uses Cloud Computing Information Resources.

WAN – Wide Area Network.

Wearable Computing Device – miniature electronic devices worn by the bearer on top of or under clothing. Examples include smartwatches, touch screens, head mounted displays, and similar devices.

# V. Enforcement

Any Staff 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 Staff members with access to ABC Company’s Information Resources.

**Policy History**

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