IT Policies Handbook

Acceptable Use Policy (AUP)

Outlines acceptable and prohibited uses of company-provided technology resources such as computers, internet, email, and mobile devices.

Password Policy

Specifies password creation guidelines, expiration frequency, and multi-factor authentication requirements to ensure secure access.

Data Protection & Privacy Policy

Covers how sensitive data (PII, financial, client data) must be handled, stored, encrypted, and sharedaligning with regulations like GDPR or HIPAA.

Access Control Policy

Defines user roles and levels of access to systems, data, and applications. Includes procedures for onboarding/offboarding and periodic access reviews.

Information Security Policy

Outlines the companys security measures, responsibilities of employees, and how incidents are to be reported and escalated.

Email & Communication Policy

Regulates appropriate use of email, instant messaging, and video conferencing platforms for business communication.

Bring Your Own Device (BYOD) Policy

Provides rules for employees who use their personal devices for work-related tasks, including security controls and monitoring expectations.

Software Installation & Usage Policy

Restricts unauthorized software installation and promotes use of licensed, approved applications to

reduce security risks.

Remote Work Policy

Defines secure remote work practices, VPN usage, and responsibilities for safeguarding company assets while working off-site.

Incident Response Policy

Details steps employees must follow in case of data breaches, cyberattacks, or system failures, including whom to contact and how to document incidents.

IT Asset Management Policy

Describes the process for tracking, issuing, returning, and retiring IT equipment such as laptops, servers, and peripherals.

Backup and Disaster Recovery Policy

Specifies backup schedules, storage locations, and recovery procedures to minimize downtime and data loss in the event of a system failure.

Internet Usage Policy

Sets boundaries for browsing, social media usage, streaming, and content filtering on company networks.

Patch Management Policy

Describes timelines and responsibilities for installing software updates, patches, and hotfixes on operating systems and applications.

Mobile Device Management (MDM) Policy

Covers the control, encryption, and wiping of mobile devices connected to corporate data.

Vendor & Third-Party Access Policy

Provides guidelines for managing external vendors' access to internal systems or data and outlines due diligence practices.

Cloud Usage Policy

Outlines the appropriate use of cloud platforms (e.g., AWS, Azure, Google Cloud) including data residency, access, and monitoring practices.