# **Overview**

**Purpose**

{COMPANY-NAME} is entrusted with the responsibility to provide services to clients who provide us with confidential information. Inherent in this responsibility is an obligation to provide strong protection against theft of data and all other forms of cyber threats.

The purpose of this policy is to establish standards for the base configuration, and acceptable use of equipment and any software running on it that is owned and/or operated by {COMPANY-NAME} or equipment that accesses {COMPANY-NAME}’s internal systems.

Effective implementation of this policy will reduce the risk of unauthorized access to {COMPANY-NAME} proprietary information and technology and protect confidential client information.

**Scope**

This policy applies to equipment owned and/or operated by {COMPANY-NAME}, and to employees connecting to any {COMPANY-NAME}-owned network domain or cloud applications that are used as part of projects or assignments managed by {COMPANY-NAME}.

# **Network/Server Security**

**Server Configuration Guidelines**

The most recent security patches must be installed on all systems as soon as it is feasible to do so, the only exception being when immediate application would interfere with business requirements.

Servers should be physically located in an access-controlled environment or a cloud infrastructure environment with an IT infrastructure provider that has achieved and maintains a high level of compliance with IT standards such as ISO-27001.

Servers are specifically prohibited from being operated from locations without appropriate physical access controls.

**Security-Related Events**

Security-related events will be reported to the IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

Evidence of port-scan or any other type of service scanning.

Evidence of unauthorized access to privileged or non-privileged accounts.

Service interruptions, error messages, or other anomalous occurrences such as that are not related to specific applications on the host.

**Router Security**

The administrator password on the router must be kept in a secure encrypted form in the location specified by the IT management. IT management must be notified of any changes to the administrator password as soon as it is feasible to do so.

The following types of traffic should be disallowed using in the firewall configuration:

* IP directed broadcasts
* Incoming packets at the router sourced with invalid addresses such as RFC1918 address
* TCP small services
* UDP small services
* All source routing

Access rules are to be added only to meet the requirements of the network topography to sustain business operations. All changes made to the access rules of network devices must be documented in the location specified by IT management. The documentation must include the date and time that the changes were made and a detailed description of the process, including any shell commands executed to make the changes.

Each router must have the following statement posted in clear view: “UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement.”

**Server Malware Protection**

*Anti-Virus* - All servers MUST have an approved anti-virus application installed and activated that offers real-time scanning protection to files and applications if the server meets one or more of the following conditions:

* Non-administrative users have remote access capability
* The system is a file server
* Share access is open to this server from systems used by non-administrative users
* Any service access is open from the Internet
* The {COMPANY-NAME} IT department deems it necessary.

**Mail Server Anti-Virus**

If the target system is a mail server it MUST have either an external or internal anti-virus scanning application that scans all mail and file attachments destined to and from the mail server.

All anti-virus applications must have automatic updates enabled and the status of automatic updates must be periodically verified. If automatic updates are not being successfully applied, IT management must be notified immediately.

**Notable Exceptions**

Exceptions to above requirements may be deemed acceptable with proper documentation if one of the following notable conditions applies to this system:

* The system is a SQL server
* The system is used as a dedicated mail server
* The system is not a Windows based platform

All on premises servers, routers, and other network appliances MUST be directly powered by a UPS (battery backup) appliance that can adequately provide surge protection and alternative power in case of power interruption. All UPS appliances should be tested annually and verified to be able to provide at least 20 minutes of alternate power source.

# **Workstation Security**

**Authorized Users**

Appropriate measures must be taken when using workstations to ensure that exposure of sensitive information is restricted to authorized users.

**Safeguards**

{COMPANY-NAME} will implement appropriate physical, administrative, and technical safeguards for all workstations that access data or information that is confidential or sensitive to restrict access to only authorized users.

**Appropriate measures include:**

* Restricting physical access to workstations to only authorized personnel.
* Configuring screen-locks to automatically lock the screen after 10 minutes of inactivity, and requiring personnel to manually enable screen-lock on workstations prior to leaving the area to prevent unauthorized access.
* Providing personnel with documentation for all password policies and procedures, and verifying personnel compliance said password policies and procedures as defined by IT management.
* Ensuring workstations are used for authorized business purposes only.
* Creating a documented list of authorized software applications for each classification of workstation determined by job requirements performed with that workstation, and providing personnel with this list that pertains to their role. Compliance should be verified by ensuring that no unauthorized software applications are installed on workstations.
* Storing all confidential or sensitive information on network servers or authorized cloud resources whenever possible.
* Applying full-disk encryption to all workstations and laptops that must store confidential or sensitive information as determined by IT management.
* Securing laptops that contain confidential or sensitive information by using cable locks or locking laptops up in drawers or cabinets when not in use.
* Anti-Virus - All workstations and laptops MUST have an approved anti-virus application installed and activated that offers real-time scanning protection to files and applications.
* All anti-virus applications must have automatic updates enabled and the status of automatic updates must be periodically verified. If automatic updates are not being successfully applied, IT management must be notified immediately.
* Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to hinder public viewing.
* Ensuring workstations are left on but logged off in order to facilitate after-hours updates. Exit running applications and close open documents.
* Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
* If wireless network access is used, ensure access is secure by following the Wireless Access policy.

**Software Installation**

Employees may not install software on {COMPANY-NAME}’s computing devices operated within the {COMPANY-NAME} internal network without explicit approval by IT management.

Installed software must be selected from an approved software list, maintained by the IT department, unless no selection on the list meets the requester’s need. The IT department will obtain and track the licenses, and test new software for conflict and compatibility before it is approved.

This policy covers all computers, servers, and other computing devices operating within {COMPANY-NAME}'s internal network.

**Malware Protection**

Anti-Virus - All {COMPANY-NAME} computers must have approved anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date.

Virus-infected computers must be removed from the network until they are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into {COMPANY-NAME}'s internal network (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, and anyone caught in violation of this policy will be criminally prosecuted to the fullest extent of the law.

# **Password Security**

**Requirements**

All system-level passwords (Administrator, etc.) must be changed on a quarterly basis, at a minimum. Technical controls should be used when possible to prevent the reuse of passwords. Technical controls should be used whenever possible to prevent the reuse of passwords, and enforce minimum password complexity.

All user-level passwords (e.g., e-mail, web, desktop computer, etc.) must be changed at least every six months. Technical controls should be used whenever possible to prevent the reuse of passwords, and enforce minimum password complexity.

All user-level and system-level passwords must conform to the standards described below in part b.

**Standards**

Password policy should be provided to all users at {COMPANY-NAME} in order to create awareness of how to select strong passwords.

*Strong passwords have the following characteristics:*

* Contain at least one of each of the following character classes:
  + Lower case characters
  + Upper case characters
  + Numbers
  + “Special” characters (e.g. @!.',#$%^&\*()\_+|~-=\`{}[]:”;’<>/ etc)
* Have a minimum length of 12 characters
* A password manager must be used to generate a pseudo random password that conforms to the above characteristics of an arbitrary length between 12 and 30 characters. All personnel must use the password manager to store passwords and make them available on all desktop, laptop, and mobile devices.

**Protective Measures**

* Do not share {COMPANY-NAME} passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential {COMPANY-NAME} information.
* Passwords should never be written down or stored anywhere online except in a password manager application that has been deemed acceptable by IT managers.
* Do not reveal a password in e-mail, chat, or other electronic communication.
* Do not speak about a password in front of others.
* Do not hint at the format of a password (e.g., “my family name”).
* Do not reveal a password on questionnaires or security forms.
* If someone demands a password, refer them to this document and direct them to the IT Department.
* Always decline the use of the “Remember Password” feature of native applications such as browsers, and web-applications.
* Multi-factor authentication (MFA) MUST be enabled on all accounts that provide such a feature, and MFA codes MUST be stored in an MFA authenticator mobile application that has been deemed acceptable by IT managers. MFA backup codes should also be stored in a password manager to ensure their security, and if MFA backup codes are provided via a downloaded file, that file must be deleted, and purged from the trash-bin of the device.

**Passphrases**

Access to the {COMPANY-NAME} internal network via remote access is to be controlled using either a one-time password (OTP) authentication or a public/private key system with a strong passphrase.

An acceptable passphrase is subject to the same requirements and limitations as account passwords which are stated above in Section IV items b and c.

# **Acceptable Use**

**General Use and Ownership**

* The data created on the {COMPANY-NAME} corporate systems remains the property of {COMPANY-NAME}.
* Any information deemed to be confidential or sensitive by {COMPANY-NAME} management, team leaders, or IT management should be encrypted following the section VI Encryption or as otherwise provided instructions from management.
* For security and network maintenance purposes, authorized individuals within {COMPANY-NAME} may monitor equipment, systems and network traffic at any time.

**Security and Proprietary Information**

* The information contained on {COMPANY-NAME}’s systems should be classified as either confidential, sensitive, or public, as defined by corporate confidentiality guidelines. Employees should take all necessary steps to prevent unauthorized access to confidential and sensitive information.
* Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
* All desktops, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, and by logging-off when moving beyond direct visual contact with the device.
* All desktops, laptops and workstations used by the employee that are connected to the {COMPANY-NAME} internal network, whether owned by the employee or {COMPANY-NAME}, shall have approved virus-scanning software configured to scan all incoming files and complete a complete device scan once per week with a current virus database unless overridden by departmental or group policy.
* Employees must use extreme caution and common sense when opening e-mail attachments received from unknown senders, which may contain various types of malware that can negatively impact {COMPANY-NAME}'s devices or network.

**Unacceptable Use**

The following activities are prohibited. The lists below are not exhaustive, but attempt to exemplify activities which fall into the category of unacceptable use.

* Under no circumstances is an employee of {COMPANY-NAME} authorized to engage in any illegal activity as defined under local, state, federal or international law while utilizing {COMPANY-NAME}-owned resources.
* Violations of the rights of any person or corporation such as defamation, liable, trademark, copyright, patent or other intellectual property, trade secret, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by {COMPANY-NAME}.
* Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which {COMPANY-NAME} or the end user does not have an active license is strictly prohibited.
* Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
* Introduction of malicious programs into the network or server (e.g., viruses, ransomware, or other malware, etc.).
* Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
* Using any {COMPANY-NAME} device or network connection to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user’s local jurisdiction.
* Making fraudulent offers of products, items, or services originating from any {COMPANY-NAME} account.
* Activity that leads to security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not authorized to access.
* Port scanning or security scanning is expressly prohibited unless prior permission is granted by IT management.
* Executing any form of network monitoring which will intercept data not intended for the employee’s host, unless this activity is approved by the IT management and deemed part of the employee’s normal job/duty.
* Circumventing or altering the normal user authentication process or security of any host, network or account.
* Interfering with or denying service to any user including the employee’s own host (for example, denial of service attack).
* Using any program/script/command, or sending messages of any kind, with the intent to interfere with any local network hosts or services or any external hosts or services via the Internet ,whether or not they are owned and operated by {COMPANY-NAME}.
* Providing information about, or lists of, {COMPANY-NAME} employees, internal hosts, or network configuration to parties outside {COMPANY-NAME}.
* Otherwise altering host or network configuration, or broadcasting any network communication data other than what is considered part of the employee's job/duty.

**Wireless Access**

*Device Requirements* - All wireless devices that reside at a {COMPANY-NAME} site and connect to a {COMPANY-NAME} internal network must:

* Be installed, supported, and maintained by the IT department.
* Use {COMPANY-NAME} approved authentication protocols and infrastructure.
* Use {COMPANY-NAME} approved authentication protocols, which may include the installation and use of RSA private and public key certificates to enable WPA2-Enterprise authentication.
* Provide the device's manufacturer issued media access control hardware address (MAC address) to the IT department to whitelist the device for access to {COMPANY-NAME} wireless network.
* Maintain the original manufacturer issued media access control hardware address (MAC address) of the device.

**Home Wireless Device Requirements**

* Wireless devices used at the employee's home such as WiFi routers, that are used in the process of accessing the {COMPANY-NAME} internal corporate network, must conform to the security protocols as detailed in sections IV Password Security and VIII Remote Access.

# **Encryption**

**Standards**

Proven, standard algorithms should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. Encryption algorithms that are considered weak by IT security industry standards should not be used, and disabled in all applications.

* Key bit strength must be at least a minimum of 2048-bit keys for RSA public / private keypairs.
* Symmetric encryption for data-in-transit and data-at-rest must use AES 256-bit keys unless otherwise specified by IT management.
* {COMPANY-NAME}’s allowed encryption algorithms and key length requirements will be reviewed annually and upgraded as technology allows.

**Mobile Device Encryption**

* Scope - All mobile devices containing stored confidential or sensitive data owned by {COMPANY-NAME} must use an approved method of encryption to protect data at rest such as full-disk encryption or application specific encryption as described below. Mobile devices are defined to include laptops, tablets, and smartphones.
  + *Laptops* - Laptops must employ full disk encryption with an encryption package approved by IT management. No {COMPANY-NAME} data may exist on a laptop in cleartext.
  + *Tablet and smartphones* - Any {COMPANY-NAME} data stored on a smartphone or tablet must be saved to an encrypted file system using an encryption package approved by IT management. All {COMPANY-NAME} tablets and smartphones shall also employ remote wipe technology to remotely disable and delete stored data in case of emergency such as a lost or stolen device.
* Keys - All keys used for encryption and decryption must meet complexity requirements described in {COMPANY-NAME}’s Password Security policy.

# **E-mail**

**Prohibited Use**

{COMPANY-NAME} e-mail system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any e-mails with this content from any {COMPANY-NAME} employee must report the matter to their supervisor immediately.

The following activities are strictly prohibited for e-mail, telephone, or any other messaging service or application:

* Sending unsolicited messages, including the sending of “junk mail”, "spam", or other advertising material.
* Any form of harassment, whether through language, frequency, or size of messages.
* Fraud, identity misrepresentation, or forging of e-mail protocol header information.
* Any communication that is not related to {COMPANY-NAME}’s products, projects, or services.
* Using non-{COMPANY-NAME} e-mail accounts (i.e., Gmail, Hotmail, Yahoo), or other external resources to conduct {COMPANY-NAME} business.

**E-mail Retention**

* Administrative Correspondence - {COMPANY-NAME} Administrative Correspondence includes, though is not limited to clarification of established policy, including holidays, time card information, dress code, workplace behavior and any legal issues such as intellectual property violations. All e-mail with the information sensitivity label Management Only shall be treated as Administrative Correspondence. {COMPANY-NAME} Administration is responsible for e-mail retention of Administrative Correspondence.
* Fiscal Correspondence - {COMPANY-NAME} Fiscal Correspondence is all information related to revenue and expense for {COMPANY-NAME}. {COMPANY-NAME}'s finance department is responsible for all fiscal correspondence.
* General Correspondence - {COMPANY-NAME} General Correspondence covers information that relates to customer interaction and the operational decisions of the business. {COMPANY-NAME} is responsible for e-mail retention of General Correspondence.
* Ephemeral Correspondence - {COMPANY-NAME} Ephemeral Correspondence is by far the largest category and includes requests for recommendations or review, e-mail related to product development, updates and status reports.
* Recovering Deleted e-mail via backup Media - {COMPANY-NAME} maintains backups from the e-mail server and once a quarter a set of backups is moved to an offsite location for long-term storage. No effort will be made to remove e-mail from the offsite backups.
* Opening any e-mail that has been labeled as "spam" and placed into the "spam" is strictly prohibited. If a legitimate business related e-mail is found to be in the spam folder, it must not be opened, and the incident must be reported to the IT department for review.

**Monitoring**

{COMPANY-NAME} employees shall have no expectation of privacy in anything they store, send or receive on the {COMPANY-NAME}’s e-mail system. {COMPANY-NAME} may monitor messages without prior notice. {COMPANY-NAME} is not obliged to monitor e-mail messages.

# **Remote Access**

**Persons Affected**

All {COMPANY-NAME} employees, consultants, vendors, contractors, students, and others who use mobile computing and storage devices on the network at the {COMPANY-NAME}.

**General Standards**

It is the responsibility of {COMPANY-NAME} employees, contractors, vendors and agents with remote access privileges to {COMPANY-NAME}’s corporate network to ensure that their remote access connection is given the same consideration as the user’s on-site connection.

**Requirements**

* Secure remote access must be strictly controlled. Control will be enforced via one-time password or public/private keys with strong pass-phrases and will always be supplemented when possible with multi-factor authentication (MFA) that supplies a one-time-password to an mobile MFA authenticator application that has been approved by the IT management. For information on creating a strong pass-phrase see the section IV Password Security policy.
* At no time should any {COMPANY-NAME} employee provide their login or e-mail password to anyone, inside or outside the organization. In the case that IT support needs to access an employee's account directly, the IT support shall change the user's password using admin privileges, and after finished, will provide the user with a temporary password, which will be required to be changed when the user accesses their account.
* Remote access to the {COMPANY-NAME} internal network is only allowed by connecting directly via an employee's home internet connection provided by an authorized ISP. Under no circumstances may an employee connect to the {COMPANY-NAME} internal network by connecting via a tethered connection to another device, or from any public WiFi connections such as a restaurant or coffee shop, a library, hotel, or other publicly available WiFi networks unless explicit permission has been provided by IT management.
* When traveling for business, {COMPANY-NAME} employee's may be provided authorization to connect to {COMPANY-NAME} internal network connections from a list of approved WiFi connections such as hotel WiFi. Alternatively, an employee may be provided with a mobile device or SIM card with mobile internet access, and instructions on how they may tether their laptop, such that they can connect to the {COMPANY-NAME} internal network securely.
* Home routers used to access to the {COMPANY-NAME} internal network must meet the minimum configuration requirements described below:
  + Admin and user authentication passwords used to connect to the WiFi services on the router must meet the requirements as specified in section IV Password Security.
  + The router must be configured to use WPA-2 or WPA-3 for authentication to WiFi services. WPA (1) and WEP WiFi authentication protocols must not be used.
* Reconfiguration of a home user’s equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
* Non-standard hardware configurations must be approved by the IT department, and {COMPANY-NAME} must approve security configurations for access to hardware.
* All desktop computers, laptops and workstations that are connected to {COMPANY-NAME} internal network via remote access technologies must have approved and fully updated anti-virus software installed and configured to immediately scan all incoming files and configured to conduct a complete scan of all files on the device at least once per week.
* Personal equipment that is used to connect to {COMPANY-NAME}'s internal network must meet the requirements of {COMPANY-NAME}-owned equipment for remote access as defined by IT management. All employees will be provided with these policies when they are provisioned credentials and other information required for a remote access connection.
* Individuals who wish to implement non-standard Remote Access solutions to the {COMPANY-NAME} production network must obtain prior approval from the IT department.

**Virtual Private Network (VPN)**

*Persons Affected* - this policy applies to all {COMPANY-NAME} employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the {COMPANY-NAME} internal network.

*Connectivity* - Approved {COMPANY-NAME} employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a “user managed” service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

**Requirements**

* It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to {COMPANY-NAME} internal network by protecting any devices used to connect to the {COMPANY-NAME} internal network using all policies described in section III Workstation Security.
* VPN authentication is to be controlled using either a multi-factor authentication (MFA) one-time password provided by an approved authenticator app or another physical token based MFA device, or a public/private key authentication with a strong passphrase. The method of authentication will be approved by IT management and provided to the employee when they are provisioned credentials and other information about the VPN connection.
* When actively connected to the corporate network, VPNs will force all traffic to and from the client device over the VPN tunnel (known as a full-tunnel): all other traffic will be dropped.
* Dual (split) tunneling is NOT permitted; only one network connection is allowed.
* VPN gateways will be set up and managed by {COMPANY-NAME}’s IT department.
* All computers connected to the {COMPANY-NAME} internal network via VPN or any other technology must use the most up-to-date anti-virus software that has been approved by IT management; this includes personal computers.
* VPN users will be automatically disconnected from {COMPANY-NAME}'s internal network after thirty minutes of inactivity. The user must then login again to reconnect to the network. Pings or other artificial network processes MUST NOT be used to keep the connection open.
* The VPN concentrator is limited to an absolute connection time of 24 hours.
* Users of computers that are not {COMPANY-NAME}-owned equipment must configure the equipment to comply with {COMPANY-NAME}’s VPN and Network policies.
* Only {COMPANY-NAME}-approved VPN clients may be used.
* By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of {COMPANY-NAME}'s internal network, and as such are subject to the same rules and regulations that apply to {COMPANY-NAME}-owned equipment, i.e., their machines must be configured to comply with {COMPANY-NAME}’s Security Policies.

# **Data Retention**

**Reasons for Retention**

{COMPANY-NAME} retains only that data that is necessary to effectively conduct its business operations and activities, and to remain compliant with applicable laws and regulations.

Reasons for data retention include:

* Providing ongoing services to registered users, customer, and clients
* Compliance with applicable laws and regulations associated with financial reporting by {COMPANY-NAME} to its funding agencies and other donors
* Compliance with applicable labor, tax and immigration laws
* Other regulatory requirements
* Compliance with industry standards certification
* Investigation of a security incident
* Restoration of data from a security incident
* Intellectual property preservation
* Defense against potential litigation

**Data Retained**

{COMPANY-NAME} has set the following specifications for types of data that shall be retained:

* Website registered and non-registered guest's data will be retained as long as necessary to provide the service requested/initiated through the {COMPANY-NAME} website, unless in the case that any registered or non-registered user requests that their any collected personally identifiable information (PII) be deleted. In such a case, any PII data associated with the requesting party will be deleted as soon as feasibly possible.
* Financial information used to process payment transactions will not be retained longer than is necessary to process a single transaction. Any IDs or tokens provided by the payment gateway provider to identify a user or process recurring payments will be stored in a database field encrypted with AES-CBC with a 256-bit key and 128 bit initialization vector (IV).
* Collected data of subcontractors and vendors will be kept for the duration of the contract or agreement and then for <Duration> more years.
* Employee data will be held for the duration of employment and then <Duration> after the last day of employment.
* Financial data associated with employee wages, leave and pension shall be held for the period of employment plus <Duration>, with the exception of pension eligibility and retirement beneficiary data which shall be kept for <Duration>.
* Recruitment data, including interview notes of unsuccessful applicants, will be held for <Duration> after the closing of the position recruitment process.
* Consultant data will be held for the duration of the consulting contract plus <Duration> after the end of the consultancy.
* Board member data will be held for the duration of service on the Board plus for <Duration> after the end of the member’s term.
* Data associated with tax payments (including payroll, corporate and VAT) will be held for <Duration>.
* Operational data related to project activities, project proposals, reporting and project management will be held for the period required by {COMPANY-NAME}.

# **Data Backup**

**Daily Backups**

Backup software shall be scheduled to run nightly to capture all incremental backup data from the previous day.

* Backup logs are to be reviewed to verify that the backup was successfully completed.

**Monthly Backups**

One full copy of "off-site" backup data shall be properly labeled and stored in a secure location other than {COMPANY-NAME}’s premises at the end of each month. In case of a disaster, these off-site backups should be available for retrieval. This off-site location shall be specified by IT management.

**Physical Backups**

Data on hard drives will be backed up daily, and mobile devices shall be brought in to be backed up on a weekly basis or as soon as practical if on an extended travel arrangement.

**Documentation**

Written documentation shall be maintained and updated that are relevant to each specific personnel role in the backup procedure. These instructions shall be provided to each personnel as a reference to their role and responsibilities as they pertain to backups.

**Backup Configuration**

Backup services shall be enabled on any cloud infrastructure / VPS infrastructure used by {COMPANY-NAME}. The minimum backup configuration is as follows:

* Cloud-server backup snapshots shall be configured to maintain one full backup of each server separately at least once per week. These weekly backups shall be maintained for at least 2 months.
* Each month, one full backup snapshot will be maintained as a long-term backup. Each long-term backup shall be maintained for at least one year.
* Backup restoration process shall be tested regularly.

# **Mobile Device Data**

**Items Covered**

Mobile computing and storage devices include, but are not limited to: laptop computers, ​​plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives (also known as a "thumb-drive"), smartphones, tablets, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or {COMPANY-NAME} owned, that may connect to or access the information systems at the {COMPANY-NAME}.

**Risks**

Mobile computing and storage devices are easily lost or stolen, presenting a high risk for unauthorized access and introduction of malicious software to the network at the {COMPANY-NAME}. These risks must be mitigated to acceptable levels as described below:

* Under no circumstances should confidential or sensitive information be copied to a USB flash drive or other unencrypted device. Files that must be transferred between devices may be transferred via a direct e-mail or by an approved cloud-storage service via a protected URL link to the resource that requires authentication.
* If files are stored on a removable hard-disk or network attached storage (NAS) device, the device must be a self-encrypting device (SED) that is capable of encrypting all stored data with an AES algorithm that uses 256-bit key strength unless otherwise approved by IT management.

**Encryption**

Portable computing devices and portable electronic storage media that contain confidential, or sensitive {COMPANY-NAME} information must use encryption to protect the data while it is being stored.

**Database**

Databases or portions thereof, which reside on the network at the {COMPANY-NAME}, shall not be downloaded to mobile computing or storage devices.

**Minimum Requirements**:

* Report lost or stolen mobile computing and storage devices to the IT department.
* Non-departmental owned devices that may connect to the {COMPANY-NAME} internal network must first be approved by the IT department.
* Compliance with the Remote Access policy is mandatory.