# IS-20 Employee and Teleworking Policies

**20.1 Employees Policy**

<COMPANY NAME> is committed to ensuring all workforce members actively address security and compliance in their roles at <COMPANY NAME>. As such, training is imperative to assuring an understanding of current best practices, the different types and sensitivities of data, and the sanctions associated with non-compliance.

**20.2 Employment Policies**

1. All new workforce members, including contractors, are given training on security policies and procedures, including operations security, within 30 days of employment.
	1. Records of training are kept for all workforce members.
	2. Employees must complete this training before accessing production systems containing ePHI.
2. All workforce members are granted access to formal organizational policies, which include the sanction policy within 1. Information Security Policy for security violations.
3. The <COMPANY NAME> Information Security Policy and Code of Condust clearly states the responsibilities and acceptable behavior regarding information system usage, including rules for email, Internet, mobile devices, and social media usage.
	1. Workforce members are required to sign an agreement stating that they have read and will abide by all terms outlined in the <COMPANY NAME> Information Security Policy and Code of Conduct, along with all policies and processes described in this document.
	2. A Human Resources representative will provide the agreement to new employees during their onboarding process.
4. <COMPANY NAME> does not allow mobile devices to connect to any of its production networks.
5. All workforce members are educated about the approved set of tools to be installed on workstations.
6. All new workforce members are given HIPAA training within 30 days of beginning employment. Training includes HIPAA reporting requirements, including the ability to anonymously report security incidents, and the levels of compliance and obligations for <COMPANY NAME> and its Customers and Partners.
7. All remote (teleworking) workforce members are trained on the risks, the controls implemented, their responsibilities, and sanctions associated with violation of policies. Additionally, remote security is maintained through the use of VPN tunnels for all access to production systems with access to ePHI data.
8. Employees may only use <COMPANY NAME>-purchased and -owned workstations for accessing production systems with access to ePHI data.
	1. Any workstations used to access production systems must be configured as prescribed in 7.8-employee-workstation-use.
	2. Any workstations used to access production systems must have virus protection software installed, configured, and enabled.
	3. <COMPANY NAME> may monitor access and activities of all users on workstations and production systems in order to meet auditing policy requirements #8.-auditing-policy.
9. Access to internal <COMPANY NAME> systems can be requested using the procedures outlined in 7.2-access-establishment-and-modification. All requests for access must be granted by the <COMPANY NAME> Security Officer.
10. Request for modifications of access for any <COMPANY NAME> employee can be made using the procedures outlined in 7.2-access-establishment-and-modification.
11. <COMPANY NAME> employees are strictly forbidden from downloading any ePHI to their workstations.
	1. Restricting transfers of ePHI is enforced through technical controls as described in 7.13-access-to-ephi.
	2. Employees found to be in violation of this policy will be subject to sanctions as described in 5.3-security-officer.
12. Employees are required to cooperate with federal and state investigations.
	1. Employees must not interfere with investigations through willful misrepresentation, omission of facts, or by the use of threats against any person.
	2. Employees found to be in violation of this policy will be subject to sanctions as described in [§5.3.3] (#5.3-security-officer).

**20.3 Issue Escalation**

<COMPANY NAME> workforce members are to escalate issues using the procedures outlined in the Employee Handbook. Issues that are brought to the Escalation Team are assigned an owner. The membership of the Escalation Team is maintained by the Chief Executive Officer.

Security incidents, particularly those involving ePHI, are handled using the process described in 11.2-incident-management-policies. If the incident involves a breach of ePHI, the Security Officer will manage the incident using the process described in 12.2-breach-policy). Refer to 11.2-incident-management-policies for a list of sample items that can trigger <COMPANY NAME>'s incident response procedures; if you are unsure whether the issue is a security incident, contact the Security Officer immediately.

**20.4** **Remote Access and Telecommuting Policy**

**Laptops and Portable Device Safeguards**

The sole reason for the allowance and use of laptops and other portable devices by authorized company personnel is to enable them to perform their job related responsibilities off of company property in remote locations.

Employees granted the use of laptop computers or other portable devices must use the following techniques to protect such equipment while in their custody and to ensure the security of confidential or sensitive information:

1. Ensure anti-virus and anti-spyware software is properly installed, enabled and continuously updated;
2. Ensure program passwords, user IDs, private encryption keys or other personal information is not automatically enabled in any way for the programs used;
3. Ensure all sensitive documents are password protected and encrypted when possible;
4. Whenever sensitive information is written to a portable storage media device it must be suitably marked with the highest relevant sensitivity classification;
5. Store back up media separately from the laptop device;
6. Enable password protected screen savers to avoid accidental exposure of potentially confidential or sensitive information;
7. Do not leave the laptop unattended in any situation, and place it in a secure location when not in use to prevent unauthorized disclosure;
8. If traveling, the equipment must remain in the possession of the user as hand luggage at all times;
9. Exercise caution with laptops in airports, especially at security screening checkpoints;
10. All media is to be stored in a locked safe, furniture or a similarly secure location when not in use; and
11. Immediately report lost or stolen laptops to the Information Technology Department.
12. Only connect to wireless networks using WPA2 encryption, a VPN should be used on all wireless networks and devices should not be discoverable by other devices on the network.

When accessing the company’s network via VPN, employees must use a company owned device. Personal devices are not permitted to access the company’s network via VPN. This is due to the fact that the company doesn’t have control over the security of personally owned devices.

**Authentication of Remote Users:**

Remote access to <COMPANY NAME> computers and networks requires that all users be definitively authenticated with dynamic passwords or other identification systems approved by the Director of Information Technology. All remote users must connect to the Company’s computers and internal networks via authorized communications systems such as firewalls and VPN’s. Two factor authentication is required for all remote access sessions.

**Location security:**

The security of <COMPANY NAME>’s information and physical property at remote locations is just as important as it is in the office. All the same security requirements apply at remote locations, although they may be implemented in different ways. For example, paper-based Confidential and Highly Restricted information needs to be locked up when not in active use. In the Company’s offices, a file cabinet might be used, but on the road, a locking briefcase might be employed.

**Authorized Software:**

All portable and remote computers which are under the control of <COMPANY NAME>, and which are used to process the Company’s business information must be protected from the installation of unauthorized software. The company shall employ processes to detect the presence of unauthorized software on company owned devices.

**Personal Firewalls – Anti-Virus Protection:**

Personal firewalls, Host Based Intrusion Detection and/or anti-virus protection should be deployed on all computers remotely accessing <COMPANY NAME>’s networks. Examples of these products include Windows Firewall, Sophos, etc. The configuration of these devices or applications is designated by the System Administrators.

**Handling Of Sensitive Information:**

In general, sensitive (Confidential and Restricted) information should not leave <COMPANY NAME> devices or networks. If it is necessary to remove computer-readable sensitive information from the Company’s offices, this information must be protected with encryption facilities approved by the Information Security Officer. Likewise, if sensitive information is transmitted over public computer networks such as the Internet, this transmission must take place with appropriate encryption facilities.

**20.5 Mobile Device Policy**

Mobile devices are important tools for <COMPANY NAME> and their use is supported to achieve the goals of the business. However, mobile devices also represent a significant risk to information and data security. If appropriate security procedures are not applied, these devices can be a conduit for unauthorized access to the organization’s data and IT infrastructure. This can subsequently lead to data leakage and system infection.

<COMPANY NAME> has a requirement to protect its information assets in order to safeguard its customers, reputation and employees.

It is the intent of this policy to protect the security and integrity of <COMPANY NAME>’s data and technology infrastructure. All <COMPANY NAME> employees must agree to the terms and conditions set forth in this policy in order to be able to connect mobile devices to the company’s network.

All mobile devices, whether owned <COMPANY NAME> or owned by employees, that have access to the company’s networks, data and systems, not including corporate IT-managed laptops. This includes smartphones and tablet computers.

**Acceptable Use**

* The company defines acceptable business use as activities that directly or indirectly support the business of <COMPANY NAME>.
* The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading.
* Employees are prohibited from accessing non-business related websites during work hours and while connected to the organization’s network at the discretion of the company.
* Devices’ camera and/or video capabilities are disabled while on-site.
* Devices may not be used at any time to:
	+ Store or transmit illicit materials
	+ Store or transmit proprietary information belonging to another company
	+ Harass others
	+ Engage in outside business activities
	+ Photocopy non-public information or customer and company data
	+ Etc.
* Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.
* <COMPANY NAME> has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

**Devices and Support**

* Only Apple iPhone and Google Android devices are allowed;
* Tablets including iPad and Android are allowed;
* Approved smartphones and tablets must be on up-to-date mobile operating system releases;
* Connectivity issues are supported by IT; employees should not contact the device manufacturer or their carrier for operating system or hardware-related issues; and
* Devices must be presented to IT for proper job provisioning and configuration before they can access corporate resources.

**Security**

* In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong pin or appropriate biometrics used to authenticate users.
* The device must lock itself with a password or PIN if it’s idle for five minutes.
* Devices must be encrypted and remain so in order to synchronize with the company network
* After five failed login attempts, the device will lock for a period of 30 seconds. Contact IT to regain access.
* Rooted (Android) or jail broken (iOS) devices are strictly forbidden from accessing the network.
* Applications must only be installed from official platform-owner approved sources; Google Play / iTunes
* Devices must have anti-virus/anti-malware software installed
* Employees are prohibited from downloading, installing and using any app that is not required for business use.
* Devices must not be connected to a PC which does not have up-to-date and enabled anti-virus/malware protection and which does not comply with corporate policy.
* Smartphones and tablets belonging to employees that are for personal use only are not allowed to connect to the network.
* Users may must be cautious about combining of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify IT immediately.
* The employee’s device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of the company’s data and technology infrastructure.

**Risks/Liabilities/Disclaimers**

* While IT will take every precaution to prevent the employee’s personal data from being lost in the event it must remote wipe a device, it is the employee’s responsibility to take additional precautions, such as backing up email, contacts, photos, etc.
* The company reserves the right to disconnect devices or disable services without notification.
* Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
* The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company’s acceptable use policy as outlined above.
* The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
* <COMPANY NAME> reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

**BYOD Program**

* <COMPANY NAME> grants its employees the privilege of purchasing and using smartphones and tablets of their choosing at work for their convenience under our Bring-Your-Own-Device or BYOD Program. Employees participating in the BYOD Program will abide by the same policies and procedures outlined above. <COMPANY NAME> reserves the right to revoke this privilege for noncompliance to this program.

**Liabilities and Responsibilities**

* The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company AND personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
* <COMPANY NAME> accepts no liability for lost employee data and will not backup personal data.
* Employees participating in the BYOD Program are responsible for notifying their mobile carrier AND <COMPANY NAME>’s IT department immediately upon loss of a device.
* <COMPANY NAME> makes no promises of privacy of employee personal data residing on the employee’s mobile device.

**Purpose**

The purpose of this Policy is to define standards for the hiring, onboarding and ongoing guidance of orgaanizational members.

**Scope**

This policy applies to all <COMPANY NAME> employees, contractors, vendors and agents with a RevSpring owned or personally-owned computer or workstation used to connect to the Company network. This policy applies to remote access connections used to do work on behalf of RevSpring, including reading or sending email and viewing intranet web resources. Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, DSL, VPN, SSH, and cable modems.

**Applicable Standards**

Applicable Standards from the HITRUST Common Security Framework

* 02.e - Information Security Awareness, Education, and Training
* 06.e - Prevention of Misuse of Information Assets
* 07.c - Acceptable Use of Assets
* 09.j - Controls Against Malicious Code
* 01.y - Teleworking

Applicable Standards from the HIPAA Security Rule

* 164.308(a)(5)(i) - Security Awareness and Training

# **Revision History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description of changes** |
|  |  | **Initial creation** |
|  |  |  |
|  |  |  |