HITRUST

POLICY TEMPLATE TOOLKIT

HITRUST POLICY TEMPLATE TOOLKIT SAMPLE POLICIES AND PROCEDURES

WWW.SHOP.FLANK.ORG

Insert Company Logo

TABLE OF CONTENTS

Insert Company Logo

Teleworking *Policy and Procedures*

Policy

[Company name] is to ensure that all applicable users adhere to the following policies for purposes of complying with the mandated organizational security requirements set forth and approved by management:

Teleworking & Telecommuting Rights

Teleworking & telecommuting, herein referred to in this policy and procedures document, is a privilege granted to employees for helping promote efficiencies in the workplace, while still maintaining quality and consistency with one's work roles and responsibilities. Teleworking is a work place environment protocol that is fully embraced by [company name] because many employees can increase productivity with teleworking, and often employees require such flexibility as traditional working hours and places of business are not conducive. Teleworking thus means to work from the employee's home or from an office near the employee's home, rather than from the main place of employment.

Teleworking is not for everyone, and is not deemed to be a reward for work performance, rather, a useful platform for which users can continue to perform their daily roles and responsibilities. For any employee to be considered for teleworking, authorized personnel at [company name] are to assess the impact of teleworking in regards to an employee's overall productivity. Specifically, this means taking in to account an employee's job functions, such as the ability for teleworking to continue to allow such job functions to be performed at optimal levels, the ability to effectively communicate with an employee, the prospects of an employee continuing to grow and learn as necessary, along with other factors deemed important for [company name].

Physical Security Environment

While [company name] will not confine an employee to a specific teleworking location, it is critical that for each location to be used, adequate physical security controls are to be in place for protecting both the employee and all relevant assets (i.e., computer, etc.) used while teleworking. Best practices measures relating to physical security are to consist of the following:

- Working in areas that allow employees an adequate degree of privacy from any other individuals, such that no eavesdropping or any other type of malicious social engineering tactics can be initiated.
- Ensuring that employees can safely exit and escape in a reasonable timeframe from any physical and or environmental threat posed.
- Ensuring the appropriate access controls are in place for securing the teleworking environment, such as traditional lock and key, punch code, electronic access control system, etc.
- Ensuring that appropriate heating, ventilation, and air-conditioning (HVAC) elements are in place.
- If necessary, and do to the sensitivity to the work being performed at the teleworking environment, appropriate security and monitoring controls are to be in place. Thus, "security" and "monitoring" implies that the facility has in place the following physical security and environmental security controls:

    - Constructed in a manner allowing for adequate protection of the teleworking environment.
    - Security alarms that are active during non-business hours, with alarm notifications directly answered by a third-party security service or local police force.
    - The use of cages, cabinets, or other designated, secured areas for securing the specified information system.
    - Access control mechanisms consisting of traditional lock and key, and/or electronic access control systems (ACS), such as badge readers and biometric recognition (i.e., iris, palm, and fingerprint

scanners/readers). Furthermore, all electronic access control mechanisms are to record all activity and produce log reports that are retained for a minimum of [x] days.
    - Adequate closed-circuit monitoring, video surveillance as needed, both internally and externally, with all video kept for a minimum of [x] days for purposes of meeting security best practices and various regulatory requirements.
    - Appropriate fire detection and suppression elements, along with fire extinguishers placed in mission critical areas.
    - Appropriate power protection devices for ensuring a continued, balanced load of power to the specified information system, thus mitigating power surges and spikes.

- [Company name] personnel have the right to inspect one's teleworking environment as necessary, yet will provide reasonable notice.
- Upon inspection, [company name] reserves the right to make any necessary changes to the teleworking environment.
- The teleworking environment is to adhere to all necessary physical security and environmental security requirements as mandated by applicable laws, regulations, client and contractual requirement, etc.

Communications and Information Security Requirements

Some of the best practices to use for ensuring the CIA triad of Confidentiality, Integrity, and Availability is upheld at all times is Defense-in-Depth and Layered security - essentially utilizing various resources for helping protect one's teleworking environment. Defense-in- Depth – for purposes of information security – includes the following layers, which have been loosely adopted and agreed upon by industry leading vendors and other noted organizations:

- Data
- Application
- Host
- Internal Network
- Perimeter
- Physical
- Policies, Procedures, Awareness

Layered security, often mentioned in the context of Defense-in-Depth, is a concept whereby multiple layers of security initiatives are deployed for the purposes of protecting an organization's critical information systems, such as one's teleworking environment. Specifically, by utilizing a number of security tools, protocols, and features, organizations can effectively put in place layers of security that – in the aggregate – help ensure the confidentiality, integrity, and availability (CIA) of systems. As such, employees that telework are to ensure that all communications and information security requirements for teleworking have adopted the concepts of Defense-in-Depth, and Layered Security.

Remote Access

Remote access is often necessary for an employee to perform his/her respective job functions, and as such, the following initiatives are to be in place:

- The [company name] remote access platform is to consist of communication protocols, and other supporting devices the ultimately ensure the confidentiality, integrity, and availability of such connections, along with the organization's network.

- The use of remote access is a privilege - one that is to be assigned only to authorized individuals with a justified business need for such access - and only after comprehensive analysis and subsequent approval procedures have been undertaken by applicable supervisory personnel and all necessary I.T. authorities.

- Unique usernames and passwords that meet or exceed stated best practices for complexity rules are to be implemented for all users with remote access rights. Also, stated lockout times for idle remote access sessions, along with predefined time parameters (i.e., 180 minutes, etc.) for allowing such access rights are to be configured accordingly.

- Two-factor authentication, which requires use of two (2) of the following three (3) methods of access – something you know, something you have, something you are – is to be incorporated as necessary for compliance purposes, specifically for that of PCI DSS compliance, HIPAA, and many other legislative mandates and industry specific directives.

- It is the responsibility of [company name] I.T. personnel to ensure that all information systems that facilitate and administer remote access rights are current with all applicable security upgrades and patches.

- Should a user suspect or confirm that an actual security issue has arisen relating to one's remote access session, such user is to terminate the remote access session and report the incident immediately to authorized I.T. personnel.

- Remote access is a privilege; thus, all authorized users are to utilize such services for business use only, with no personal or questionable activities allowed. "Business use only" implies the following: (1). for facilitating all required duties for a stated job function, (2). for communicating with other authorized parties (i.e., employees, clients, contractors, etc.), (3). for conducting research applicable to one's job duties.

- [Company name] reserves the right to monitor one's remote access sessions without consent, which may include installing agent software on end-user systems for a variety of security, performance, and overall monitoring issues.

- Personal and confidential information is never allowed to be stored on any local devices used for enabling a remote session, such as one's hard drive, or using external storage devices via USB connections.

Remote Access Security Measures

Because of the different types of remote access mediums and protocols allowed, along with the numerous devices that can be used for initiating remote access sessions, the following security measures apply:

- Remote access client software – if residing on a user's device – is not to be altered in any way.
- Personal firewall software must be enabled on computers, along with other malware protection measures, such as a current, known, and stable version of anti-virus.
- Along with not altering remote access client software, users are also forbidden from altering and changing any configurations on [company name] information systems that would affect the security of such systems, and also the remote access session.
- Users are forbidden from initiating remote access sessions from untrusted end-user devices that are not owned, operated, maintained, and controlled by [company name] and pose a serious security threat. Common examples include the following: mall kiosks that offer Internet services, hotel business |

computer rooms offering PC's for use, office supply | mailing stores providing computers for printing, faxing, scanning services, etc.

- Users are forbidden from engaging in dual connectivity | concurrent connectivity, whereby user is connected to the [company name] network, while also on another network.
- Remote access rights are strictly for authorized users who have been assigned such rights, and not for any other individuals, such as personal friends, family members, co-workers, etc.
- Confirmation of remote session termination, such as closing out of the program and the browser, is to be conducted after each session. As a security precaution, [company name] has implemented a pre-determined "time-out" clause for remote access to helping increase security.

In summary, the same consideration that is given to a user's onsite connection to the [company name] network must also be utilized for remote access sessions. Additionally, users are to display reasonable and prudent security measures for ensuring the physical safety of any [company name] devices for establishing remote access sessions. This would include not leaving laptops in untrusted environments, safely securing devices when in public domains, etc.

Security Parameters for Unauthorized Access

Only authorized personnel are to access the teleworking environment; thus family, friends, and other relevant personnel are to be restricted from gaining access to such facilities. While many teleworking environments outside of an employee's home are that of shared office space, please ensure that all teleworking equipment is thus secured at all times. When at home, please ensure best practices are in place for ensuring unauthorized access is not allowed, thus locking doors and securing teleworking equipment when not in use is.

Intellectual Property

Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce. Therefore, [company name] IP is protected in law by patents, copyright and trademarks, which enable [company name] to earn recognition or financial benefit from what they invent or create. **Source: http://www.wipo.int/portal/en/.**

As such, any [company name] IP accessed, used, and developed on non-company information systems (i.e., privately owned information systems) is fully owned and controlled by [company name]. Furthermore, for additional information on IP, please contact authorized personnel within [company name].

Access to Equipment

At any time, with or without notice, [company name] has the right to access any information systems and other supporting devices (i.e., equipment) being used by an employee while teleworking for [company name]. While the nature for accessing such equipment is largely for preventative maintenance and security patching, other reasons may also be warranted. As such, employees are to provide full cooperation and access to equipment as needed by authorized personnel within [company name].

Malware Protection and Network Security Requirements

Anti-virus and anti-malware solutions utilized by [company name] employees that telework must be from an approved vendor, one that offers ongoing customer support pertaining to the installation and maintenance of the applicable software. Specifically, this includes all necessary installation documentation (i.e., manuals, user administrator and setup guides, hardening guides, etc.), "virus support" initiatives, such as providing updates for new detection signatures and the applicable dictionaries, etc. Simply stated, whatever computer an employee is using for teleworking, it needs to have current, updated anti-virus on it. This is one of the most fundamentally important - and easy to implement - security safeguards as it protects your computer from malware and other malicious exploits.

Additionally, a personal firewall is to be used as this provides an additional layer for helping protect a teleworking employee's home network in the following manner: (1). Protects the user from unwanted incoming connection attempts, ultimately allowing the user to control which programs can and cannot access the Internet. (2). Blocks and/or alerts a user about outgoing connection attempts. (3). Monitors and regulates all incoming and outgoing Internet users.

Type of Work Permitted

Activities performed by employees that are teleworking are to be strictly associated with their respective job functions, roles and responsibilities such employees have been assigned to. While [company name] understands that personal activities do occur during work related hours – such as answering personal emails, taking personal calls, etc. – employees are nonetheless to spend their time performing work related duties as their primary function.

During defined teleworking hours, which is to consist of normal business hours as described by [company name] human resources, employees are to have access to whichever internal systems at [company name] are needed to perform their work-related duties. When connecting to internal systems at [company name], only approved protocols are to be used for ensuring the confidentiality, integrity, and availability (CIA) of the remote access session.

Suitable Equipment

All equipment used by employees teleworking must be approved by authorized personnel at [company name] for ensuring it is both appropriate and sufficient for work use. Equipment can include all types of information systems and other supporting devices necessary for one to perform their respective job duties. Non-approved equipment, regardless of how safe, secure, or efficient such systems may be, are not to be used at any time by teleworking employees.

Furthermore, equipment is allowed to be inspected at any timey by authorized personnel at [company name], and users are not allowed to modify and/or disable any configurations on equipment without prior approval. All equipment owned by [company name] is to be returned in good working order if an employee no longer is teleworking, or that employee has been voluntarily or involuntarily terminated from [company name].

Family and Visitor Access

Only authorized personnel are to be allowed to access the actual space for which a [company name] employee is teleworking. Because many employees will be teleworking from home, it is important to work in an area that is safe and secure in that only an employee can physically access the designated area during normal business hours. Once such normal business hours are over, then all teleworking equipment is to be secured as necessary, especially if the area then becomes a place where friends and family members may visit. As for teleworking at other locations other than one's home, [company name] employees are to use their discretion and best judgement regarding who can access the facility being used and in what capacity.

Hardware and Software Support and Maintenance

All equipment used by [company name] employees while teleworking, are to maintain up-to-date hardware and software as necessary. For hardware, this means using approved equipment that allows employees to work securely and efficiently. For software, this means ensuring that equipment has current patches and security updates installed, along with license agreements allowing the use of such software on equipment.

Additionally, at any time, [company name] authorized personnel are to be able to access all hardware and software for performing necessary support and maintenance activities for ensuring the safety and security of such equipment.

Insurance

Appropriate insurance is to be maintained for all teleworking equipment used by employees of [company name]. The legal department within [company name] maintains all information pertaining to insurance coverage, therefore, any questions regarding insurance for teleworking equipment is to be addressed to such personnel as needed.

Backups and Business Continuity

While teleworking, [company name] employees are to save information while connected to the network, thereby allowing such data to be ultimately saved with the backup process being performed by authorized I.T. personnel. Employees are forbidden from saving information on equipment (i.e., desktops, laptops, etc.), as such devices could be easily destroyed during a disaster.

[Company name] employees that are teleworking are to also ensure that adequate Business Continuity and Disaster Recovery (BCDRP) initiatives are in place for ensuring the safety and security of individuals, along with the ability to continue operations in the event of a disaster. [Company name] has in place a documented BCDR plan, for which all employees have been provided a copy as necessary. As for employees that are teleworking, each employee is to provide an assessment of the physical location for which they are teleworking, and what BCDRP initiatives are in place. This process is to include communication with authorized personnel at [company name] for ensuring such a plan is acceptable and documented.

Audit and Security Monitoring

At any time, [company name] may employee all necessary audit and security monitoring tools and techniques for helping ensure the safety and security of data and information being accessed at the teleworking environment for which employees are located. Additionally, at any time, [company name] may employee all necessary audit and security monitoring tools and techniques for helping ensure the safety and security of teleworking equipment owned by [company name]. Common audit and security monitoring initiatives include the following:

- **Configuration and Change Monitoring:** The use of specialized software, such as File Integrity Monitoring (FIM), Host based Intrusion Detection Systems (HIDS), and/or change detection software programs are to be implemented for monitoring servers as they provide the necessary capabilities for assisting in the capture of necessary events. Additionally, configuration change monitoring tools are to be used to detect any file changes made within a specified information system, ranging from changes to commonly accessed files and folders, to more granular based data, such as configuration files, executables, rules, and permissions.
- **Performance and Utilization Monitoring:** Additional measures are to be employed for ensuring that information systems are actively being monitored for all necessary performance and utilization measures, such as the following: (1). CPU Utilization. (2). Memory Utilization. (3). Disk Utilization.

Revocation of Teleworking & Telecommuting Rights

At any time, [company name] has the right to implement revocation procedures regarding teleworking for any employees. Any number of factors could lead to such rights being revoked, ranging from performance and security issues to operational and financial constraints. When such measures are put in place, [company name] employees are to assist authorized personal as necessary.

Information Security Sanction & Disciplinary Process *Policy and Procedures – Personal Data*

Policy

[Company name] is to ensure that all applicable users adhere to the following policies for purposes of complying with the mandated organizational security requirements set forth and approved by management:

Information Security Sanction & Disciplinary Action – Personal Data

Ensuring the safety and security of Personal Data is one of the most tasks any employee or contractor can undertake for [company name]. With today's increasing reliance on information technology for all types of business related procedures, Personal Data must be safeguarded at all times, both in electronic format and hard-copy, paper based documents. The ability to successfully ensure the safety and security of Personal Data for [company name] is highly dependent upon understanding what PII is.

With regards to REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, "**Personal Data**" is defined as: *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

Source: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Unacceptable Uses of Personal Data

As such, any misuse, abuse, and harmful activities that result in Personal Data being compromised will not be tolerated at any time by [company name], and will result in necessary sanctions being taken against such individuals. More specifically, the unauthorized access, use, and/or disclosure of Personal Data is a serious issue, one that will be aggressively enforced at all times by authorized personnel within [company name] consisting of reprimanding, suspending and/or terminating such individuals. Accessing Personal Data is a privilege, one granted to select users for performing one's respective job functions, thus all necessary security safeguards are to be implemented at all times for protecting highly sensitive and confidential data.

Thus, any action resulting from the unauthorized access, use and disclosure of Personal Data that may potentially compromise the organization's network infrastructure, cause harm to other related systems, cause harm or pose a significant financial, operational, or business threat to the organization because of inappropriate and unacceptable access, use, and disclosure of Personal Data, will result in swift sanctions to be applied to such individuals.

The following Levels are to be assessed against employees regarding unauthorized access, use, and disclosure of Personal Data:

Level 1: Mistaken | Accidental Access, Use, and/or Disclosure of Personal Data

- **Level 1 Violation specific to** Personal Data**:** Any employee or other applicable user who mistakenly accesses, uses, and/or discloses Personal Data. This may range from accidentally accessing electronic and/or hard-copy Personal Data, such as computer records, paper records, etc., to the following:
    - Mistakenly accessing Personal Data for which a user (i.e., employee, contractor, vendor, guest, etc.) does not need to access for one's job.
    - Mistakenly leaving a workstation unattended that may contain Personal Data.
    - Mistakenly copying Personal Data without proper approval by authorized personnel.
    - Mistakenly changing Personal Data without proper approval by authorized personnel. Such change may include actual changes to Personal Data resident within [company name] information systems.

- Mistakenly discussing Personal Data in a public forum or public venue that could lead to another individual obtaining such information.
- Mistakenly discussing information with unauthorized personnel.
- Mistakenly harming and or/destroying [company name] owned, operated, and/or maintained information systems – both hardware and software.
- Any other mistaken or accidental unauthorized access, use, and disclosure of Personal Data and/or actions identified by [company name] that could impact the safety and security of the organization's information systems.

- **Level 1 Reprimand and Disciplinary Action:** (1). Written warning, (2). along with undertaking specific security awareness training procedures within thirty (30) days of the reported violation. Please note that if the mistaken or accidental unauthorized access, use, or disclosure of Personal Data was so severe that it impacted [company name] materially, then immediate termination is to undertaken. Additionally, please note that multiple instances of Level 1 violations will result in reprimanding, suspending and/or terminating such individuals. Please See Level 3 Violations for more details.

- **Note:** Accidents do happen, and [company name] is understanding of such issues, but also the need for ensuring all employees know what information they can and cannot access.

Level 2: Deliberate and Intentional Access, Use, and/or Disclosure of Personal Data

- **Level 2 Violation specific to Personal Data:** Any employee or other applicable user who deliberately and intentionally accesses, uses, and/or discloses Personal Data. This may range from knowingly accessing electronic and/or hard-copy Personal Data, such as computer records, paper records, etc., to include the following:
  - Deliberately and intentionally accessing Personal Data for which a user (i.e., employee, contractor, vendor, guest, etc.) does not need to access for one's job.
  - Deliberately and intentionally leaving a workstation unattended that may contain Personal Data.
  - Deliberately and intentionally copying Personal Data without proper approval by authorized personnel.
  - Deliberately and intentionally changing Personal Data without proper approval by authorized personnel. Such change may include actual changes to PII data resident within [company name] information systems.
  - Deliberately and intentionally discussing Personal Data in a public forum or public venue that could lead to another individual obtaining such information.
  - Deliberately and intentionally discussing information with unauthorized personnel.
  - Deliberately and intentionally harming and or/destroying and [company name] owned, operation, and/or maintained information systems – both hardware and software.
  - Any other deliberate or intentional unauthorized access, use, and disclosure of Personal Data and/or actions identified by [company name] that could impact the safety and security of the organization's information systems.

- **Level 2 Reprimand and Disciplinary Action:** (1). Immediate termination, with no exceptions, unless in the interest of national security. (2). Possible criminal charges and penalties.
  - **Note:** Deliberate and intentional access, use, and/or disclosure of Personal Data, will not be tolerated at any time, ultimately resulting in the immediate termination of such individuals.

Level 3: Multiple Infractions of Level 1 Violations of Access, Use, and/or Disclosure of Personal Data

- **Level 3 Violation specific to Personal Data:** Any employee or other applicable user who mistakenly accesses, uses, and/or discloses Personal Data for any second or subsequent occurrences of Level 1 Violations. This may range from accidentally accessing electronic and/or hard-copy Personal Data, such as computer records, paper records, etc. Specific examples include the following:
    - Mistakenly accessing Personal Data for which a user (i.e., employee, contractor, vendor, guest, etc.) does not need to access for one's job.
    - Mistakenly leaving a workstation unattended that may contain Personal Data.
    - Mistakenly copying Personal Data without proper approval by authorized personnel.
    - Mistakenly changing Personal Data without proper approval by authorized personnel. Such change may include actual changes to Personal Data resident within [company name] information systems.
    - Mistakenly discussing Personal Data in a public forum or public venue that could lead to another individual obtaining such information.
    - Mistakenly discussing information with unauthorized personnel.
    - Mistakenly harming and or/destroying [company name] owned, operated, and/or maintained information systems – both hardware and software.
    - Any other mistaken or accidental unauthorized access, use, and disclosure of Personal Data and/or actions identified by [company name] that could impact the safety and security of the organization's information systems.

- **Level 3 Reprimand and Disciplinary Action:** (1). Immediate termination, with no exceptions, unless in the interest of national security. (2). Possible criminal charges and penalties.

- **Note:** While accidents do happen, and [company name] is understanding of such issues, multiple occurrences – those beyond the first occurrence – will not be tolerated.

It's important that all employees and other workforce members are aware of the sanctions that can be imposed on them for unintentionally, carelessly, or deliberately accessing, using, and/or disclosing Personal Data. The safety and security of consumer information and our information systems is of the utmost priority for the organization, thus [company name] will enforce such sanctions aggressively.

Return of Assets *Policy and Procedures*

Policy

[Company name] is to ensure that all applicable users adhere to the following policies for purposes of complying with the mandated organizational security requirements set forth and approved by management:

Scope of Assets

In terms of assets, [company name] is to ensure the proper return of the following items. This is not an all-inclusive list, rather, a starting point to use:

- Computer (Laptop)
- Printer, Scanner, Fax
- Cell Phone, Pager
- Portable Digital Assistant (PDA)
- USB Drives, External hard Drives, etc.
- Company Credit Card
- Access Devices-Keys
- Access Devices-Electronic Badges | Swipe Cards
- Furniture
- Pictures
- Uniforms
- Parking Permits

Company Owned Assets

All information systems owned, operated, maintained and controlled by [company name] are deemed to be the sole property of the organization. As such, company assets in the possession of individuals (i.e., employees, contractors, etc.) are to be surrendered upon termination – either voluntarily or involuntary termination – from [company name]. Additionally, if an individual has legally acquired an asset from [company name], such as through a purchase – the assets is to be examined for ensuring no sensitive and unauthorized company and/or client data resides on the asset. If information is found, then the asset is to be seized with appropriate sanitization methods performed.

Assets Owned by Individuals

Likewise, if an individual is using his/her own asset, such as a laptop or any other type of computing system for conducting business activities, then the asset is to be examined by authorized I.T. personnel within [company name] prior to the individual's termination. As with [company name] owned assets, assets owned by individuals are to be examined for ensuring no sensitive and unauthorized company and/or client data resides on the asset. If information is found, then the asset is to be seized with appropriate sanitization methods performed.

Access Control *Policy and Procedures*

Policy

[Company name] is to ensure that all applicable users adhere to the following policies for purposes of complying with the mandated organizational security requirements set forth and approved by management:

Security Requirements of Business Applications

Business applications are any software applications/systems developed internally by [company name] and/or acquired from vendors that are critical for the organization's operations. These applications are essential to assisting [company name] in performing all necessary financial, operational, technical, and security functions, and must be protected accordingly. One of the first layers essential to protecting such applications is ensuring that only authorized users have access to them, which ultimately means a structured, formalized provisioning process is to be in place.

Additionally, once provided access, users are only to be given the minimum access needed to perform their respective job duties, a concept known as Role Based Access Control (RBAC). The subsequent policies and procedures stated herein are to be applied to all business applications regarding access and other essential information security best practices.

Information Dissemination and Authorization

All information pertaining to access rights and other information security best practices is to disseminated in a complete and timely manner to all in-scope users of [company name] information systems. In doing so, [company name] is ensuring that clarity and transparency are provided in regards to the overall confidentiality, integrity, and availability (CIA) of the organization's information systems.

The dissemination practice requires that [company name] develop and distribute complete, accurate, and relevant information security policies and procedures, those pertaining to access rights and other essential information security best practices. Ultimately, the proper dissemination of policies allows for the understanding and subsequent enforcement rules for what the relevant domains within information security, such as access rights, and others.

Security Levels and Classification of Information & Consistency of Access Rights

Access rights to [company name] information systems, and ultimately to data and information, is to align with the organizations' relevant classification of information policies, procedures, and processes. This means that for the type of data and information for which [company name] has identified and labeled, an associated description of what types of access rights allowed to such data and information is to be documented.

This ultimately ensures that access rights to data and information is commensurate with the assigned classification and information levels provided by the organization. This type of consistency of access rights in regards to data and information being accessed ultimately helps ensure the confidentiality, integrity, and availability (CIA) of [company name] property.

Legislation and Contractual Obligations for Data Access Rights

Access rights to [company name] information systems are to meet all applicable legislative, compliance, contractual, and other necessary mandates for ensuring the safety and security of data and information systems for which the organization is authorized to store, process, transmit, and/or access. Select personnel within [company name] are to identify, assess, implement, and continuously monitor all obligations regarding the access of data, and what restrictions – if any – are imposed on limiting access to such data. This requires authorized I.T. personnel within [company name] to put in place access control restrictions as necessary, along with employing continuous monitoring initiatives for ensuring compliance is being met.

Management of Access Rights

Access rights to [company name] information systems is to include having a clear, concise, and complete understanding and awareness of all systems for which users can access, particularly with environments that are distributed, often extending beyond the organization's Local Area Network (LAN). For all connection points in and out of [company name]'s network, the associated access control points are to be fully documented as necessary for ensuring a complete understanding the types of access allowed.

Segregation of Access Controls

It is the policy of [company name] that no single user or single group is to be allowed to hire, provision, modify, and terminate access for users. Such duties are to be effectively segregated for helping ensure the safety and security of [company name] information systems.

Access to Networks and Network Services

Only authorized users are to access network and network services. Users of [company name] networks and network services include both administrators that manage the networks, and end-users that rely on such services. As such, the following matrix provides essential information regarding access to [company name's] networks and network services:

ENVIRONMENT: Description of networks and network Services to be Accessed:	The ABC data analytics service offering is a Software as a Service (SaaS) based platform hosted in Amazon AWS and offered to clients through a secure web-browser SSL link for which they can access their own system and perform numerous backend permissions, such as adding and removing users, generating reports, and other as needed functions.
INFORMATION SYSTEMS: Description of the networks and networks services architecture:	The ABC Data Analytics SaaS platform consists of three (3) virtual firewalls, two (2) virtual switches, one (1) load balancer, and twenty-five (25) virtual servers, with three (3) web servers, eight (8) application servers, two (2) database servers, and twelve (12) other various production and development servers – all Linux based and hosted in the AWS cloud at Amazon.
AUTHORIZATION PROCEDURES: Description of authorization procedures of who is allowed to access the networks and networks services:	Describe how the authorization procedures regarding access to the networks and network services.
MANAGEMENT CONTROLS: Description of management's controls for protecting access to the networks and networks services:	Describe management's controls for protecting access to the networks and network services.
ACCESS MECHANISMS: Description of tools/utilities/protocols for accessing networks and network Services to be Accessed:	Describe what tools/utilities/protocols are used regarding access to the networks and network services.
USER AUTHENTICATION: Description of authentication requirements for accessing networks and networks services:	Describe the authentication requirements regarding access to the networks and network services.
MONITORING: Description of monitoring of the networks and networks services:	Describe what "monitoring" initiatives are in place regarding access to the networks and network services.

User Registration and De-Registration

Throughout the access control lifecycle, appropriate naming schemes and supporting logic are to be developed and implemented, resulting in an identity (i.e., username) that assigns all users their own unique identifier, thereby minimizing the chance of duplication of any employee's given identification credentials. Moreover, naming schemes are not to be a reflection of one's roles or responsibilities within the organization, such as using the titles given to actual users that have elevated or privileged rights or names of critical environments (i.e., super user, root, production, development, etc.) as their actual naming scheme.

Furthermore, [company name] is to also implement any necessary proprietary naming schemes for ensuring the confidentiality and privacy of employee identification credentials, when necessary. Senior executives and other personnel identified by [company name] as having a valid and credible need for protecting their respective identification credentials will be granted unique usernames based on confidential naming schemes that differs from company-wide users.

As part of [company name]'s access rights policies, procedures, and processes, user IDs are to be managed for ensuring the following:

- Users are assigned unique ID's, which ultimately allows [company name] to identify and "link" to such users all actions taken by them with their respective unique ID.
- Disabling and removing user ID's for users who have left the organization.
- Ensuring that duplicate/redundant user ID's are not in use.
- Assigning unique user ID's to users who need additional layers of confidentiality, such as C-level executives.

[Please discuss in detail what specific naming schemes you have in place for all information systems within your organization and how this logic is conducive to your organization, how it also helps minimize the chance of duplication of any employee's given identification credentials (i.e., unique), along with not being descriptive in nature as to a user's role or responsibility within the organization.]

The following personnel have been identified as having a valid and credible need for protecting their respective identification credentials, and are to be granted a unique "identity" based on confidential naming schemes:

Confidential Naming Schemes Matrix

	Name	Title	Business Reason & Justification
(1).	?	Chief Executive Officer	Privacy reasons for the officer
(2).	?	Chief Financial Officer	Privacy reasons for the officer
(3).	?	Chief Operating Officer	Privacy reasons for the officer
(4).	?	Chief Information Officer	Privacy reasons for the officer
(5).	?	?	?
(6).	?	?	?
(7).	?	?	?
(8).	?	?	?
(9).	?	?	?
(10).	?	?	?

For the above referenced table, please list the names, title, and corresponding reason & justification for having a unique identity. Many times, C level officers and other designated personnel are assigned unique identities based on confidential naming conventions for protecting access to them from a wide range of individuals and entities, both internally and externally.

User Access Provisioning

Ensuring that only authorized users are granted access to [company name] information systems ultimately requires that a structured, formalized, and documented user registration, de-registration, associated user access provisioning process, and other supporting initiatives, is in place.

All users requiring access to information systems are to undergo a valid access authorization process for accessing information systems that includes documenting the name of the user, the type of access granted/intended system

usage, and the specific roles and responsibilities given to such users. A valid access authorization process can include a documented authorization form, electronic correspondence confirming provisioning of a user, or any other type of acceptable form of access authorization materials. [Company name] formally documents the user access provisioning process in the following manner: [Please describe what documentation is used for provisioning new users. *Note. we have provided a series of authorization forms for all types of users which can be used for facilitating this requirement*].

Additionally, the following access policies are to be enforced at all times:

- Access to any [company name] information systems must include authorization from the owner of the information system.
- Access rights granted are appropriate and consistent for the user.
- Access rights are not to be granted until all necessary authorization procedures are complete.
- Access rights are to be maintained for ensuring a full and documented history exists for all users accessing [company name] information systems. As such, access records exist in the following manner: [Discuss where the access rights documents are stored, for how long, who has access to them, etc.].
- Periodically, users do have their access rights modified and adapted for ensuring they continue to have the minimum necessary access to fully execute their stated job roles and responsibilities. When such access has to be modified/adapted, authorized personnel are to make all necessary system configuration changes regarding access rights, which also requires documenting the changes with all necessary forms and other associated procedures. Documentation is key for ensuring changes to access rights are justified, authorized, and implemented correctly. [Company name] formally documents the user access modification process in the following manner: [Please describe what documentation is used for modifying access rights. *Note. we have provided a series of authorization forms for all types of users which can be used for facilitating this requirement*].

Management of Privileged Access Rights

Only authorized users are to be granted privileged access rights to [company name] information systems. As for defining "privileged access rights", it is the following: A user that has been granted administrative access rights that has the ability to change, modify, delete a wide-range of elements within an information system. More specifically, privileged access rights allow a user to make changes to configuration files, delete files, and many other critical functions. Because of this, privileged access rights are to be monitored at all times, in the following manner:

Identification of Privileged Access Rights: Ensuring that privileged access rights are managed accordingly requires [company name] to identify all types of privileged access rights within all information systems, and within all environments. Authorized personnel are to complete the "Privileged Access Rights" Matrix below, completing all field as necessary for ensuring the information is valid, accurate, and complete:

Privileged Access Rights Matrix (Environment A)

Environment:	The ABC data analytics service offering is a Software as a Service (SaaS) based platform hosted in Amazon AWS and offered to clients through a secure web-browser SSL link for which they can access their own system and perform numerous backend permissions, such as adding and removing users, generating reports, and other as needed functions.			
	Listing of Privileged Access for Information Systems			
Types of Information Systems	**Type of Privileged Access**	**Description**	**Review and Expiry of Access**	**Listing of Personnel**
Firewalls	System administrator access to the firewall	These individuals with "system administrative" access to the firewalls have full capabilities for changing configuration files, system settings, adding/removing/modifying user access, and more.	Authorized personnel review access quarterly, more frequently as needed, and determine expiry date during the review	ABC Company Network Engineering team, which consists of five (5) members.
Routers				
Switches				

Production Environment Servers (Web Servers)				
Production Environment Servers (Application Servers)				
Production Environment Servers (Database Servers)				
Production Environment Servers (File Servers)				
End-Users				
?				
?				
?				

Clear Desk and Clear Screen *Policy and Procedures*

Policy

[Company name] is to ensure that all applicable users adhere to the following policies for purposes of complying with the mandated organizational security requirements set forth and approved by management:

General Awareness of One's Work Environment

Ensuring the safety and security of one's workspace environment requires a general awareness and knowledge of basic, yet essential, security best practices. Not leaving passwords on Post It Notes, securing sensitive documents in a locked cabinet when not in use; these are just a few of the security requirements that all users are to be aware of regarding the security of one's workspace. While most security practices should be inherently known, it's also important that all users undergo annual security awareness training for gaining additional knowledge on other subject matter relating to the safety and security of ones' workspace.

It's also important to note the following clear desk and clear screen requirements are to be in place wherever a user is working – at the office, at home, on the road. Keeping a "security first" mindset ultimately helps in ensuring the safety and security of [company name] assets.

Remember also that you have a shared responsibility for helping keep your co-worker's workspace areas safe and secure also. If you see something that is out-of-place and poses a possible security issue, then notify appropriate personnel immediately.

Computer Workstation Security Requirements

Your computer is one of the most important items to secure, thus the following requirements are to adhered to at all times by all users:

Computers are to be locked from a logical access control perspective when not in use. This requires initiating a screensaver on the actual computer, or completely shutting the computer down. It is the policy of [company name] to lock access to your computer when left unattended for any period of time. Even going to the restroom, taking a brief water break, or conversing with an employee in close proximity still requires you to invoke the screen saver settings that can only be unlocked with a username and password. Simply stated, if your workspace is not occupied by you, then you need to logically and physically secure your computer.

If your computer is not physically taken with you at the end of your work day, then it is to be shut down completely, which means completely powering down the device and not leaving it in "sleep" or "hibernate" mode.

Physical Security Requirements

Computers, if left overnight, must be cable locked or put in a safe place. All other confidential material and items must be securely locked in a file cabinet, etc. Workstations must be left clear and free of any type of items deemed a target by somebody looking to obtain valuable or sensitive information about you, our business, or our clients. The less you leave at your workstation, the better.

Sensitive Information

Company data, personal data, client data – anything deemed sensitive or confidential (i.e. printouts, documents, folder, CD ROMS, etc.) – is to be safely secured at all times when one's workspace is unattended. Such materials should therefore be secured in file cabinets and/or any other location deemed safe and secure. Remember, our clients expect and demand that their information is safe and secure at all times, so think before you leave something unattended at your workspace.

Presentation Materials

Any presentation materials used that showcase/illustrate sensitive information is to be removed/cleared from one's workspace when unattended. Whiteboards are one of the most common examples as individuals often use them for "data flowing" sensitive processes and information. "Erase at all times" is the motto to adopt for white boards.

Storage Devices

Removal hard drives, memory sticks, external USB thumb drives – any type of removal storage device – are to secured at all times when one's workspace is left unattended. Such devices often contain highly sensitive information and are never to be left unattended. Such devices should therefore be secured in file cabinets and/or any other location deemed safe and secure. Take them with you or store them safely somewhere, but never leave them unattended at a workspace.

Unique Identification Information

Passwords, passphrases, social security numbers, dates of birth, client login information – these are just a few examples of the many types of "Unique Identification Information" that should never be left unattended at one's workspace. Often, this information is found on a Post It Note or some other type of sticky pad, which is a clear violation of this stated policy. If you cannot remember some type of unique identification information, then store the credentials in a secure physical space or on your workstation computer where it is safe and secure.

Physical Access Devices

Traditional keys, key FOBs, electronic access control system (ACS) badges – these are also just a few examples of the many types of "Physical Access Devices" that should never be left unattended at one's workspace. An individual with malicious intent can very easily grab such items and immediately begin trying to access rooms, facilities, or other secure locations. Such devices should therefore be secured in file cabinets and/or any other location deemed safe and secure. Take them with you or store them safely somewhere, but never leave them unattended at a workspace.

Secure Disposal of Information

For any items that must be discarded from one's workspace – from paper based documents to electronic devices – approved disposal methods are to be used, such as incineration, pulverizing, shredding, degaussing, secure wipe, etc. Just because it leaves your workspace, you cannot assume it has been safely disposed of, thus ensure proper protocols are in place for such initiatives.

Printers and Photocopiers & Other Reproduction Technology

Reproduction Technology – such as printers, photocopiers, scanners, digital cameras, etc.) are only to be used in a manner consistent with guidelines provided by the organization. This means using best practices and sound judgement when using any of these technologies.

End-of-Workday Protocols

All individuals should strive to implement the following end-of-workday protocols regarding clear desk and clear screen requirements:

- If your workstation computer is not going with you, then ensure it is completely powered down and physically secure via a cable or some other type of physical security apparatus.
- Look around and gather all physical items that need to be locked away or taken with you. If you're not sure as to the sensitivity of an item, secure it or take it with you.
- For any documents that need to be disposed of, place them in a secure shredding bin, or, if allowable, shred them yourself.
- Scan your workspace one final time for ensuring you've secured your area as best as possible.

Non-Compliance

Please note that non-compliance with the aforementioned policies and procedures will result in any of the following disciplinary measures:

- Initial Notification and Warning
- Second Notification and Warning
- Loss of Privileges
- Suspension
- Termination

Separation of Development, Testing, and Operational Environments *Policy and Procedures*

Policy

[Company name] is to ensure that all applicable users adhere to the following policies for purposes of complying with the mandated organizational security requirements set forth and approved by management:

SoD – Information Systems

SoD for information systems is essential for helping ensure the safety and security of [company name]'s information systems. More specifically, SoD is an I.T. "best practice" that assists in ensuring the confidentiality, integrity, and availability (CIA) of [company name]'s information system landscape. With increasing data security threats facing [company name], both internally and externally, it is vitally important to separate duties accordingly for ensuring no single user or group of users have complete control over any type of information security lifecycle.

Additionally, SoD applies to all environments within [company name], such as development, staging, and production, and is to include appropriate access controls for ensuring users have the minimum acceptable level of access necessary for performing his/her respective job function. Compensating controls are to be used as necessary when a complete separation of duties is not feasible.

Information Security Duties and User Departments & Users of Systems

Information security duties are to be segregated from the actual user department & user of information systems as this helps prevent fraud, error and misuse of information systems. While user departments & user of systems are to provide meaningful input regarding information systems, it is not their responsibility to perform any relevant security duties. Specifically, security duties that should be segregated from use departments & users of systems are to include the following:

- Provisioning information systems.
- Establishing access rights and removing access for users assigned to information systems.
- Installing patches and other necessary security updates to information systems.
- De-commissioning and/or removing information systems from production.
- Changing configuration settings on information systems.
- Changing, modifying, disabling applications or other features currently in use.

Development, Testing and Production/Operational Environments

Separating development and testing environments from production/operational environments is one of the most essential elements for SoD regarding information systems. Users that develop and/or test systems and applications are not to have access to production/operational environments as unauthorized changes can create numerous issues that could ultimately harm [company name]'s information systems, such as un-approved changes to systems and files, along with possible failure of such systems.

As such, separating development and test environments from production/operational environments helps to ensure accidental and unauthorized changes that could affect the confidentiality, integrity, and availability (CIA) of [company name] information systems. The following mandates are to be implemented regarding SoD for development, testing and production/operational environments:

- Development and testing environments access rights are to be separated from production/operational environments.

- Development and testing personnel are not to have access to systems in production/operational. When such SoD are not fully allowed, then compensating controls are to be implemented and enforced at all times.
- Different access control log-on initiatives are to be implemented for helping reduce the risk of error, such as using different usernames and passwords for development and testing environments and for production/operational environments.
- In such instances where a clear separation of personnel exists between development/testing environments and production/operational environments, there is never to be a co-mingling of activities between such environments.

Development/Testing and Production/Operational Environment Matrix

Name of System	Development/Testing Environment Description and SoD Controls	Production/Operational Environment and Description of SoD Controls
Online SaaS Data Analytics Portal	Developers only have access to the online SaaS DEV environment which is hosted at Amazon AWS, but on a completely different instance from the production/operational environment, and on a completely different AWS account that is logically separated from the main AWS production environment, which has its own account.	Only production personnel have access to the online SaaS data analytics production/operational environment, with developers not having any access whatsoever.

Separation of Duties Requirements	Initiatives Implemented
Rules of transfer of software from development to production/operational	Describe what your practices are regarding transferring/migrating software from development to production/operational.
Testing of Changes	Describe the change process for making changes to software while in dev/testing/staging
Reasons for Testing in production/operational	Describe what circumstances would allow for testing to be done on a production/operational environment.
Restriction of Development Tools	Describe how the production/operational environment restricts access to development tools – compilers, editors, etc.
User Profiles for Different Environments	Describe what practices are in place for ensuring users have different user profiles for the various environments.
Use of Sensitive Data	Describe how sensitive data, if used, is protected during testing.

Development and I.T. Operations

Individuals responsible for developing, testing, and migrating information systems (i.e., applications and other supporting modules and I.T. systems) are to be segregated from I.T. operations. "I.T. Operations" are the personnel that perform the following duties:

- Data Entry
- Support Services
- I.T. Infrastructure and Operations

In essence, individuals using the information systems are those prohibited from developing, changing, and maintaining the information systems.

Database Administrator and I.T. Administrative Duties

Separating database administrator (DBA) duties from that of I.T. and platform specific administrative duties is essential for helping reduce fraud, error, and misuse of information systems. As such the following SoD are to be applied regarding separating duties between DBA functions and I.T. Administrative duties and functions:

- Revoke and/or remove external stored procedures permissions.
- Disallow I.T. Administrators to have any type of DBA access rights credentials.
- Prohibit the use of mixed-code authentication to databases.
- Do not allow the database to be installed via local I.T. admin accounts.
- DBA level access to production/operational databases is prohibited for any personnel that also have system software level access, or application developer access.
- Ensure that the following roles and responsibilities are effectively segregated at all times:
    - Database Administrator
    - Server Administrator
    - Backup Operator
    - Security Administrator

Information Transfer *Policy and Procedures*

Policy

[Company name] is to ensure that the all applicable users adhere to the following policies for purposes of complying with the mandated organizational security requirements set forth and approved by management:

Transfer of Information

Information being transferred through the use of all types of communication facilities must be protected at all times. With growing cybersecurity threats, all personnel are to be aware of the organization's information transfer policies, procedures, and processes. The ultimate goal when transferrin information is to ensure the confidentiality, integrity, and availability (CIA) of the data being sent and/or received by [company name]. This in turn requires the use of numerous industry approved data transmission protocols, along with supporting software solutions that are to be used at all times.

From a procedures perspective, information transfer activities are to be done so with approved data transmission protocols, using approved systems. Depending on the type of data being sent, various protection methods are to be used, ranging from encryption to password protecting files, and other necessary mechanisms. Additionally, [company name] has in place numerous acceptable uses policies that guide users on various aspects of sending and receiving data. Furthermore, authorized personnel at [company name] are to configure a deploy network tools and solutions that aid and assist in such endeavors for the protection of information transfer. Together, these procedures, help information from being intercepted, copied, modified, misrouted, and/or destroyed.

Protection Against Malware

[Company name] mail servers are to be configured will all necessary mail anti-malware solutions, such as antivirus and anti-spam, along with other essential utilities for effectively blocking and containing email born viruses and other malware threats. Specifically, all email communications and web browsing for webmail must be sent through the applicable email filtering systems for ensuring file extensions that are known to contain malware, such as .vbs, .dat, .exe, .pif. .scr, are blocked. Additionally, many commonly used file extensions can also contain malware, thus use caution at all times when opening, saving attachments, or forwarding them also.

Protection of Attachments

Attachments, which are often sent with emails, are to be protected if the information is deemed sensitive in nature. Please refer to [company name]'s data classification matrix to determine the classification of data and if the attachment needs to be protected. Two (2) methods are to be used for protecting attachments, either (1). Password protection, or (2). Encryption. All attachments, regardless of format (i.e., zip file, pdf, Microsoft Word, photos, etc.) must thus either be encrypted or password protected. Please refer to the actual tool or solution used for the relevant procedures.

Acceptable Use of Communication Facilities

The following guidelines, for which all personnel are to receive copies on and acknowledge, provide guidance and acceptable usage rights regarding [company name]'s communication facilities and related assets:

- Laptop Usage Policy and Procedures
- Information System Usage Policy and Procedures
- Internet Usage Policy and Procedures
- Software Usage Policy and Procedures

User Responsibilities

The following guidelines, for which all personnel are to receive copies on and acknowledge, provide guidance on specific unacceptable behavior, specifically, the following: defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.

- Laptop Usage Policy and Procedures
- Information System Usage Policy and Procedures
- Internet Usage Policy and Procedures
- Software Usage Policy and Procedures
- E-Mail Usage Policy and Procedures

Cryptographic Techniques

[Company name] is to utilize encryption standards as designated by the "Federal Information Processing Standards (FIPS), which consist of publicly announced standardization documentation developed by the U.S. government and issued by the National Institute for Standards and Technology (NIST). Specifically, **FIPS 140-2** | Security Requirements for Cryptographic Modules and **FIPS-197** | Advanced Encryption Standard (AES) form the basis of approved encryption standards and strengths for all products and protocols used by [company name] regarding confidentiality and integrity of data.

Other standards and best practices that provide encryption guidance, such as those advocated by the **The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)**, are to be utilized also. The GDPR is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

Additionally, cryptographic protocols are to be utilized for data transmission activities over untrusted networks, which include, but are not limited to, the following:

- **IPSec:** Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet within the actual communication session.
- **TLS | SSL:** Transport Layer Security (TLS) and Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet utilizing both asymmetric and symmetric cryptography.
- **SSH:** Secure Shell (SSH) is a cryptographic network protocol for secure data communication between two networked computers that connect through a secure channel over an insecure network, a server and a client.

Cryptographic Protocol in Use	Description	Business Justification for Use
IPSec	Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet within the actual communication session.	
TLS | SSL	Transport Layer Security (TLS) and Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet utilizing both asymmetric and symmetric cryptography.	
SSH	Secure Shell (SSH) is a cryptographic network protocol for secure data communication between two networked computers that connect through a secure channel over an insecure network, a server and a client.	
?		
?		

?		

Retention and Disposal Guidelines

Data retention and disposal guidelines are outlined specifically within [company name]'s **Protection of Records Policy and Procedures** which provides detailed information regarding as to the types of data kept and the relevant disposal techniques used.

Controls and Restrictions on Communication Facilities

The use of communications facilities must be done so in accordance with one's roles and responsibilities at [company name]. As such, all personnel are to be aware of general best practices, which include, but are not limited to, the following:

- Limiting physical access only to areas where allowed.
- Limiting logical access only to systems allowed.
- Dressing and acting in an appropriate, professional manner at all times.
- Adhering to all stated employment requirements, acceptable usage policies, and more.

Appropriate Precautions

Ensuring the safety and security of confidential information is paramount, and as such, personnel are to never access systems for which they have not been given authorization to, never leaving information in public areas, along with employing other necessary best practices. The following guidelines, for which all personnel are to receive copies on and acknowledge, provide guidance and acceptable usage rights regarding [company name]'s regarding confidential information.

- Laptop Usage Policy and Procedures
- Information System Usage Policy and Procedures
- Internet Usage Policy and Procedures
- Software Usage Policy and Procedures
- E-Mail Usage Policy and Procedures

Answering Machines

Answering machine, if still in use, are never to store sensitive information, as it can be easily re-played and copied by an unauthorized individual. The same holds true for cellular voice mails, as such messages can also be re-played, even forwarded, to another cellular phone.

Facsimile Machines

Facsimile (fax) machines, if still in use, are to be safeguarded from the following security issues:

- Unauthorized access to built-in message stores to retrieve messages.
- Deliberate or accidental programming of machines to send messages to specific numbers.
- Sending documents and messages to the wrong number either by misdialing or using the wrong-stored number.

Public Venues

Conversing in public means being aware of the conversation one is having as other individuals can easily eavesdrop on your conversation. Be mindful of your audience and think before you speak for ensuring no sensitive information is shared.

Insert Company Logo

Download your copy of the HITRUST Policy Template Toolkit Today from Flank.