Cyber Security Controls
For MS vendors & contractors

PURPOSE

stc and its MS Vendor/contractors organization depend on the reliable functioning of its critical infrastructure. Information Security threats exploit the increased complexity and connectivity of critical infrastructure systems, placing **stc** and its MS Vendor's security, economy, and stakeholder safety at risk.

It is important that MS Vendor implements **stc**'s Information Security Baseline controls for safeguarding MS Vendor's information systems landscape, ultimately ensuring the confidentiality, integrity, and availability (CIA) of critical system resources.

The main objectives of recommending and implementing the Information Security Baseline controls are as follows:

a) Protect the Confidentiality, Integrity, and Availability of the MS Vendor data via people process and technology related controls.

b) Provide for the development, implementation, review, and maintenance of minimum-security controls required to protect the MS Vendor's data and systems.

c) Protect **stc** MS Vendor, its employees, and its clients from illicit use of company data and systems.

d) Ensure effectiveness of security controls over data and systems that support **stc** MS Vendor's operations.

e) Enhance Information security awareness on current and emerging information security risks.

f) Remain compliant to applicable legislative, regulatory, and IPR (Intellectual Property Rights) requirements.

Because each MS Vendor's risks, priorities, and systems are unique, the tools and methods used to achieve the outcomes described by the baseline may vary.

DEFINITIONS

The cyber security controls are applicable to all **stc** teams that manage **stc** Contractors, Managed Service vendors, and Third-Party Organizations.

It is the responsibility of each concerned personnel to understand the applicability of the guidelines and clarify doubts, if any, that they may have.

PROCEDURAL STEPS

CONTROL STRUCTURE

Control Number - Each control has a unique number

Control Objective - States the cyber security goal to be achieved irrespective of the implementation method

Implementation Guidance - The suggested means by which the Control Objective can be fulfilled

Examples have been included as appropriate throughout the baseline document for ease of understanding

CYBER SECURITY CONTROLS FOR stc MANAGED SERVICES VENDORS & CONTRACTORS DOCUMENT

This baseline document describes a set of mandatory security controls for **stc** MS Vendors.

Mandatory security controls establish a security baseline for the entire community and must be implemented by all MS Vendors on their local, remote, and/or cloud infrastructure. **stc** has chosen to prioritize these mandatory controls to set a realistic goal for nearterm, tangible security gain and risk reduction.

stc CYBER SECURITY BASELINE MANDATORY CONTROLS

ASSET MANAGEMENT CONTROLS

Control Type: Mandatory	**Reference ID:** ISMS-POL-04 Asset Management Policy

Control Objective:
Ensure that adequate information security controls are deployed on the information and information systems, which handle confidential information.

Implementing Guidelines:
stc MS Vendors at the most basic level should have the following controls with reference to Asset Management Security.

Control 1.1

a) Information Asset Owners and Information Custodians shall identify Assets under their control including Information (Electronic), Physical, Paper, People, Application / Software Asset and Information processing services. A formal inventory shall be maintained for all assets under their custody.
b) The loss, theft or misappropriation of assets shall be reported immediately to stc Management. Examples of Asset Types are listed in the table below:

Asset Type	Examples (not limited to)
Information (Electronic)	Database, data files, Operational & Support Documents etc.
Physical	Physical Assets like Servers, Desktops, Firewalls, Printers, Machines, Faxes, Telephone, UPS, AC etc
Paper	User Manuals, Contracts, Agreements, Operational & Support Procedures Include personnel required to support and run other assets.
People	People and their qualifications, skills, and experience
Application	Application software, system software
Software Asset	development tools, and utilities
Services	Including Computer & Communication Services and General Utilities

Control 1.2

a) Information Owners and Information Custodians shall document, maintain and verify Asset inventories periodically.

The following information shall be recorded to facilitate system Planning and Asset Recovery in the case of interruption, corruption, loss or destruction:

1. Type of Asset
2. Owner
3. Custodian
4. License Information
5. Description
6. Asset Classification
7. Asset Location

Control 1.3

All information assets shall be listed and maintained in an information asset inventory that is periodically reviewed :

Asset Classification and Handling:
Assets shall be classified according to their sensitivity and criticality. Appropriate handling, storage, transmission, and disposal procedures shall be applied based on the classification.

Asset Lifecycle:
Asset owners are responsible for ensuring assets are securely managed throughout their lifecycle from acquisition to disposal, including secure data erasure or destruction.

ACCEPTABLE USAGE OF ASSETS CONTROLS

Control Type: Mandatory	**Reference ID:** ISMS-POL-04 Asset Management Policy

Control Objective:
Ensure to establish acceptable and unacceptable use of electronic devices and network resources at **stc** MS Vendors in conjunction with their established culture of ethical and lawful behavior, openness, trust, and integrity.

Implementing Guidelines:
stc MS Vendors at the most basic level should have the following controls with reference to Acceptable usage of assets.

Control 2.1
Rules for the acceptable use of information and of assets shall be established for the following:
- Information Assets
- Information processing facilities
- Staff using their own devices controlled under "Bring your own device" acceptable use management.

Control 2.2
a) Users shall use provided assets and other information resources strictly for legitimate business purposes, protect the confidentiality of **stc** business and information obtained in the course of performing their job.
b) **stc** Management has the right to access all information stored on any device belonging to **stc** and permissions to disable security services, devices, or software on any **stc** device shall be based on explicit authorization.
c) **stc** Management reserves the right to perform a compliance review on a periodic basis to ensure compliance with this Policy. The user shall report any observed or suspected Cyber Security incidents and/or weaknesses to the **stc** Cyber Security department.
d) Users shall not discuss with colleagues about the suspected weakness once it is reported to a higher authority for investigation.
Usage of **stc**'s resources shall be within legal boundaries.

f) Usage of workstations (Laptops / Desktops), Internet, Email/ other **stc** owned / leased / operated communication medium, portable assets, Telephony and Information systems. shall be as per defined acceptable usage.

Control 2.3
a) Users are provided with technology resources to facilitate effective, secure and ethical electronic business communications and activities.
b) Technology resources may only be used after management approval, for approved purposes and by authorized users for the sole purpose of fulfilling any assigned job responsibilities.
c) The **stc** IT team will remove any unauthorized software in end user systems.

Control 2.4
a) The users shall assign to **stc** all Intellectual Property Rights (IPR) which arise in the course of performing their obligations under the contractual agreement (including all present and future copyright, trademark and patent as well as their revivals and extensions and all Intellectual Property Rights in all IP Materials).
b) The Users and Third Parties handling Intellectual Property may only use the Intellectual Property Rights and IP Materials to perform job obligations under agreement and shall not disclose any Intellectual Property Materials to any other party without the prior written consent of the Management of **stc**.
c) The user shall immediately transfer to **stc** all IP Materials and company owned equipment in their possession or under their control when the contractual agreement expires or terminates for any reason, or at any time the company requests transfer. No copies or other record of any IP Materials may be retained by the user except with the prior written consent of **stc** Management.

Control 2.5
a) **stc** System and Application Accounts (login ID's and passwords) shall be used only for the business purpose for which they are requested and authorized. Passwords must never be shared for any reason.
b) Under no circumstances will the user account be used for participation in a personal financial activity, investment, promotional contest etc.
c) Users are responsible for protecting any information used and / or stored / accessed through their individual user accounts.
d) Users shall not divulge **stc** information to anyone outside **stc** without proper authorization. All information made available to the user in their business capacity will be considered as 'Internal' unless expressly stated otherwise.
e) Users shall not attempt to access any data or programs contained on any system for which they do not have authorization or explicit written consent of the owner of the system.
f) Electronic communication facilities (such as Email, Internet browsing) are for authorized business use only. Fraudulent, harassing or obscene messages and / or materials shall not be sent from, to or stored on **stc** systems. This Policy explicitly prohibits browsing obscene web sites / messages on the company facilities. Any violation of this will result in strict disciplinary action including contractual termination.
g) The transmission of any material that is in violation of any Kuwait law, order or regulation is prohibited.
h) Users shall not download any freeware / shareware / unlicensed software versions of software from the Internet without proper authorization and approval from the **stc** Cyber Security department.

Control 2.6
The following activities are strictly prohibited unless mentioned in this Policy:
a) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, using any tool / software to by-pass existing system controls or policies, by-pass authentications, disable logging, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties, as defined by user's management. For purposes of this Policy, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

b) Port scanning or security scanning is expressly prohibited unless prior notification to the **stc** IT Team is made and authorized by IT Team in case the Scanning is done as part of Yearly Audit Assessment.
c) Users without authorization cannot execute any form of network monitoring which will intercept data not intended for the user's host.
d) Users shall not make copies of system configuration files for their own, unauthorized use or to provide to other people/users for unauthorized use.
e) Interfering with or denying service to any user e.g. denial of service attack. Control 2.7

a) **stc** defines acceptable business use as activities that directly or indirectly support the business of **stc**.
b) **stc** defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing, if applicable.
c) Users are blocked from accessing certain websites during work hours / while connected to the corporate network at the discretion of the company.
d) 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
e) Users may use their mobile devices to access the following **stc**-owned resources: email, calendars, contacts, documents, etc.

Control 2.8

a) Smartphones including iPhone, Android and Windows phones are allowed.
b) Tablets including iPad and Android are allowed.
c) Connectivity issues are supported by the **stc** IT department.

Control 2.9

a) In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the **stc** network.
b) The **stc**'s strong password policy is: Passwords must be at least eight characters and a Combination of Alphabets (Small and Capital), Numerical, Special Characters. Passwords will be rotated every 45 days and the new password can't be one of 5 previous passwords.
c) The device must lock itself with a password or PIN during idling time based on respective device's secure lock settings.
d) After five failed login attempts, the device will lock. Users must contact the **stc** IT team to regain access.
e) Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
f) Users are automatically prevented from downloading, installing and using any app that does not appear on the **stc**'s list of approved apps.
g) Smartphones and tablets that are not on the company's list of supported devices are/are not allowed to connect to the network.
h) Users' access to **stc** data is limited based on user profiles defined by the **stc** IT department and is automatically enforced.

Control 2.10

a) The **stc** IT team will take every precaution to prevent the user's personal data from being lost in the event it must remote wipe a device.
b) **stc** reserves the right to disconnect devices or disable services without notification.
c) Lost or stolen devices must be reported to the company within 24 hours.
d) Users are always expected to use their devices in an ethical manner and adhere to the **stc**'s acceptable use policy as outlined above.
e) The user 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. **stc** reserves the right to take appropriate disciplinary action up to and including contractual termination for non-compliance with this policy.

Control 2.11

All users shall return any organizational assets in their possession upon termination of their contractual agreement.

INFORMATION CLASSIFICATION CONTROLS

Control Type: Mandatory	**Reference ID:** ISMS-POL-04 Asset Management Policy

Control Objective:
To ensure that corporate data are properly labeled to receive an appropriate level of protection.

Implementing Guidelines:
stc MS Vendors at the most basic level should have the following controls set in relation to information classification control.

Control 3.1
Information assets at **stc** shall be classified appropriately as Restricted, Confidential, and Public, based on the following metrics:

- Criticality of the information.
- Legal requirements for protection of the information.
- Value of the information.
- Sensitivity of the information.
- Confidentiality, integrity and availability requirements of the considered information. ●

The type of asset.

- The Impact of a security breach.

Control 3.2
All information assets (equipment, peripherals, software media, paper documents, information stored in computer systems) shall be labelled physically or electronically as per their classification.

Control 3.3

a) Information asset shall be handled in a manner to protect the information asset from unauthorized or accidental disclosure, modification, and/or loss.
b) Information handling, processing, storing, and communicating shall be consistent with the information classification in order to protect it from unauthorized access and misuse.

Control 3.4

a) **stc** supplied media shall only be used to store, process, transfer, dispose data or information for business purpose. b) Any media that has not been supplied by **stc** shall not be used.
c) **stc** information that is classified as "Confidential" shall be stored into encrypted on media.
d) When the media is connected to a system e.g. desktop / laptop, anti-malicious software shall be used to scan and remove computer viruses, if found.
e) Only **stc** data that are authorized and necessary to be transferred shall be saved on to the Media.
f) Special care shall be taken to physically protect the media and stored data from loss, theft or damage.
g) Access to the media shall be restricted to ensure authorized access.

Control 3.5

a) Data on media shall be erased before destroying or re-using the same.
b) Storage devices that are damaged prior to disposal may contain very sensitive data and shall require physical destruction if they cannot be securely erased.
c) Optical media should be broken or scratched when no longer required.

Control 3.6

a) Assets that are classified as 'Public' can be sent in an open mail/courier.
b) Assets that are classified as 'Confidential' or 'Company Restricted' can only be sent using trusted personnel or through courier service with whom a contract exists.

ACCESS CONTROL CONTROLS

Control Type: Mandatory	**Reference ID:** ISMS-POL-05 Access Control Policy

Control Objective:
Allowing only authorized access for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Implementing Guidelines:
stc MS Vendors at the most basic level should have the following controls with reference to Access Control.

Control 4.1 **use '.' after personnel**

Third party personnel access request to **stc** information assets and revoking shall be the responsibility of concerned project team. Access for contractors, consultants, or vendor personnel to **stc** information assets shall be provided only on the basis of a formal contract and signing of Non-Disclosure Agreement (NDA). The agreement shall provide:

- The terms and conditions under which access is provided.
- The responsibilities of the contractors, consultants or vendor personnel.
- Agreement by the contractors, consultants or vendor personnel to abide by **stc**'s Cyber Security Policy. These instructions shall include security requirements, such as the need to maintain the confidentiality of the information, requirements for distribution of the information during the period of access.

Control 4.2

Access to **stc** information systems shall be restricted to authorized users to support and enable business requirements. Access to information systems shall be controlled based on the following:

a) The Information security classification of the Asset.
b) Applicable legal and / or contractual obligation to restrict or protect access to Information Assets)
c) Access Criteria:
   - Need to Know - access is only granted to the information required to perform a role, and no more.
   - Need to Use - Users will only be able to access physical and logical facilities required for their role.
   - Defense in Depth - security must not depend upon any single control but be the sum of a few complementary controls.
   - Least Privilege - the default approach taken must be to assume that access is not required, rather than to assume that it is.
d) Access to Information Assets and activation of user accounts for approved / authorized contractors, consultants, temporary workers, or vendor personnel shall be controlled and only be in effect when the individual is actively performing service with **stc**.
e) Remote access to **stc**'s network and resources will only be permitted provided that authorized users are authenticated, and privileges are restricted.
f) Access to Operating System commands shall be restricted to those persons who are authorized to perform systems administration functions.
g) Access shall be granted while ensuring segregation of duties to avoid 'conflict of interest'.
h) Segregation of duties shall be ensured in development, testing and production environments.

Control 4.3

a) Access to network services shall be granted as needed to support business requirements.
b) Network access must be restricted to the authorized users and systems, using the principle of least privilege.

Control 4.4

a) Remote users shall connect to **stc** Network only through approved and designated remote access services and secure gateways and require user identification and authorization.
b) **stc** provides VPN facility for users based on business requirements and with appropriate approvals.

Control 4.5

Access to information resources will be managed using multiple types of accounts, including:

a) Regular Accounts - Provide personnel with the minimum level of information resources and system functionality needed to perform their duties and do not carry special privileges above those required to perform the business function.
b) Privileged / Administrator Accounts - Provide higher levels of access for individuals who perform system administration and User Account Maintenance functions or personnel who administer restricted information resources.
c) Privileged accounts shall be used in accordance with the following guidelines:
   - Assignment must be restricted to personnel whose duties require additional privileges.
   - Privileged accounts must be assigned to a unique individual.
   - Administrator shall not use 'Administrator', 'Admin', 'root', 'superuser' or similar names for privileged accounts as User-Id for performing administrative activities in Servers / Databases / Network devices etc. Privileged IDs should not be named such that the access rights of the account is explicitly identifiable and may be permissible only where the regular user-id usage has limitations / restrictions or due to operational issues.

Control 4.6

Users should be required to sign a statement to keep personal secret authentication information confidential and to keep group (i.e. shared) secret authentication information solely within the members of the group; this signed statement may be included in the terms and conditions of the contractual agreement.

Access Review:
Access rights shall be reviewed at least quarterly by the asset owners to ensure access remains appropriate and unnecessary privileges are revoked

Multi-Factor Authentication:
MFA shall be enforced for all remote access, privileged accounts, and access to sensitive systems.

Logging and Monitoring:
All access and authentication events shall be logged and monitored to detect and respond to unauthorized access attempts

Temporary Access:
Temporary access may be granted under exceptional circumstances, with formal approval and automatic expiration. All temporary access shall be reviewed post-usage

Control 4.7

Removal of User accounts & access privileges of personnel leaving shall be disabled through the appropriate process before the end of the contract period, depending on their criticality of job scope

Control 4.8

Access to program source code and associated items shall be stored in the form of program source libraries segregated from operational environment. This shall ensure prevention of the introduction of unauthorized functionality and unintentional changes as well as to maintain valuable intellectual property

CRYPTOGRAPHIC USAGE CONTROLS

Control Type: Mandatory	**Reference ID:** ISMS-POL-06 Cryptographic Usage Policy

Control Objective:
To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of **stc** information, its clients and third parties.

Implementing Guidelines:
stc MS Vendors at the most basic level should have the following controls with reference to Cryptographic Usage.
Control 5.1

a) **stc** has 2-factor Authentication in place for logging on to any critical server/network and IT Infrastructure.
b) Standards and procedures shall be in place for the use of cryptographic controls in all critical IT and Network Systems to protect sensitive information of **stc**, clients and third parties.
c) Identified Assets are implemented with necessary controls to ensure the Cryptography applicability. In general, encryption techniques for the relevant business process or situation shall be adopted, as listed in the table below:

Process / Situation	Technique
Email Security	Approved Enterprise Email Solutions
Protect Passwords on Systems	Password Management Applications
Protection of Data on Storage	Endpoint Encryption
Remote Access	Virtual Private Network (VPN)
Routers	Encrypted Communication
Switches	Encrypted Communication
Firewalls	Encrypted Communication

Control 5.2

a) Cryptographic controls shall be considered for, but not limited to, the following: ● External connections.
● Confidential information shared over public and/or shared communication networks.
b) Use of cryptographic controls shall comply with all relevant laws industry leading practices and reviewed periodically for any new regulations.

PHYSICAL AND ENVIRONMENT SECURITY CONTROLS

Control Type: Mandatory	**Reference ID:** ISMS-POL-07 Physical and Environment Security Policy

Control Objective:
To deploy suitable physical and environmental security controls for the prevention of unauthorized access, compromise, theft, damage or interference to business premises, information processing facilities and telecommunication facilities.

Implementing Guidelines:
stc MS Vendors at the most basic level should have the following controls with reference to Physical and Environment Security.

Control 6.1

a) Visitors (Clients, Vendors, Suppliers, Site-visitors, Consultants and Contractors) should obtain permission before entering the Information Processing Facilities and server rooms. Temporary ID cards should be issued to **stc** visitors or guests.
b) Physical access to **stc** secure areas such as datacentre or areas where sensitive information is stored and operational control facilities exist, is restricted to prevent any unauthorized physical access.
c) No photographic, video, audio or other recording equipment should be allowed without authorization to secure areas (restricted zones).

d) Access Logging:
Electronic access control systems shall be used to manage and log entry to secure areas. Access logs must be retained and reviewed regularly.

e) Environmental Controls:
Secure areas shall be equipped with fire detection and suppression, temperature and humidity controls, and power backup to protect equipment and data.

f) Visitor Management:
Visitors must sign in and out at reception, wear visible temporary IDs, and be escorted at all times while in secure areas.

Control 6.2

a) Physical access rights to secure areas should be revoked immediately or as approved by the department head upon termination/ resignation of employees or completion of a consultation or vendor agreement.
b) Unsupervised working in secure areas by third party personnel and Vendors should be avoided both for safety reasons and to prevent opportunities for malicious activities.
c) Third party support/services personnel should be granted restricted access to secure areas only when required. These personnel will always be escorted and monitored for their activities in the secure areas. Suitable personnel will be identified to accompany housekeeping personnel during the routine cleaning of the secure areas.

Control 6.3

a) Equipment should be maintained in accordance with the supplier's recommended service intervals and specifications. Annual Maintenance Contracts (AMC) / Preventive Maintenance (PM) contracts should be entered with Vendors, where required.
b) Only authorized maintenance personnel should carry out repairs and service equipment. Activities of on-site maintenance should be supervised to ensure that the support staff does not have unauthorized access to **stc**'s data.
c) Any physical security breach or suspicious activity must be reported immediately and investigated according to incident management procedures.

OPERATIONS SECURITY CONTROLS

Control Type: Mandatory	**Reference ID:** ISMS-POL-08 Operations Security Policy

Control Objective:
To ensure correct and secure operations of information systems, those information systems are protected against malware and loss of data, that events are logged and compliance monitored, that operating system software is controlled, and that the exploitation of technical vulnerabilities are prevented.

Implementing Guidelines:
stc MS Vendors at the most basic level should have the following controls with reference to Operations Security.

Control 7.1
Development, testing and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.

Control 7.2

a) All Information Systems at **stc** including Servers, Desktops and Laptops shall have Anti- malicious solutions installed. **stc** shall deploy Anti-malicious solutions and controls at various levels as below: ● Desktop Level.
   - ● Server Level.
   - ● Critical access points / specific gateways where information from public domain ingresses into **stc**'s Network e.g. email, web traffic.

b) All viruses, Trojan horses and other malware incidents should be reported by users to the **stc** IT Service Desk. Malware-infected computers shall be removed from the network or placed in a quarantine segment as soon as they are identified, until they are verified as virus-free.

Control 7.3
System for Event logs, exceptions and security relevant events on IT and Network systems will be recorded, stored and protected based on business/regulatory requirements. Security event logs review, logging information maintenance and system administrators/ operators' logs shall be monitored. All systems connected to **stc**'s network will be time synchronized to ensure that the event logs have accurate information. Controls shall include:

- ● Physical security safeguards.
- ● Permission for administrators and operators to erase or de-activate logs.
- ● Multifactor authentication for access to critical assets where applicable.
- ● Backup of audit logs to off-site facilities.
- ● Automatic archiving of logs to remain within storage capacity.

Control 7.4
Periodic Technical Vulnerability Assessments will be conducted by the Cyber Security team or qualified external assessors under a well-defined contract and non-disclosure agreement; Identified technical vulnerabilities will be assessed for the potential risks and rectified according to the remediation plan.

Patches and updates shall be evaluated and applied in a timely manner to mitigate known vulnerabilities

Control 7.5

a) Users are not allowed to install software on **stc** devices unless specifically authorized.
b) Authorized personnel are responsible for the installation of software, updates, and patches.

COMMUNICATION SECURITY CONTROLS

Control Type: Mandatory	**Reference ID:** ISMS-POL-09 Communication Security Policy

Control Objective:
To ensure the protection of information in **stc** networks and maintain the security of information transferred within an organization and with any external entity.

Implementing Guidelines:
stc MS Vendors at the most basic level should have the following controls with reference to Communication Security.

Control 8.1

- ● Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements. When engaging with external service providers or services, outsourcing protocols as part of shall be implemented.
- ● The information services within **stc** shall be suitably segregated on the network including segregation of testing and production, separation of critical networks from the Internet and other internal, less sensitive networks with appropriate separation techniques.
- ● **stc** shall ensure that the Users of network services have segregation of duties with appropriate rights and access control.

Control 8.2
stc shall ensure policies and procedures to maintain the security of information transferred within an organization and with any external entity and shall include, but not limited to the following areas:

- Network Security Agreements
- Confidentiality Agreements
- Non-Disclosure Agreements
- Internet usage
- Email Security
- Web filters:

Email systems shall implement anti-spam, anti-phishing, and encryption capabilities to protect against common email threats.
Communication with third-party providers must be secured through contractual agreements and technical controls to protect confidentiality and integrity
All sensitive data transmitted over networks, including email and file transfers, must be encrypted using approved cryptographic standards
Acceptable use and Non-Acceptable use within **stc** Network or within organization services.

SECURE SYSTEM DEVELOPMENT LIFECYCLE CONTROLS

Control Type: Mandatory	**Reference ID:** ISMS-POL-10 Secure System Development Lifecycle Policy

Control Objective:
To ensure that information security is an integral part of information systems across the entire lifecycle including services over public networks, security measures to protect the application and application source code, during systems design, development and maintenance and protection of data during testing.

Implementing Guidelines:
stc MS Vendors at the most basic level should have the following controls with reference to Secure System Development Lifecycle.

Control 9.1
Outsourced software development shall be supervised and monitored by **stc** through NDA, Risk Assessment, Contractual agreements, Management Review meetings whichever applicable.

Access to source code repositories shall be restricted and logged, with encryption used to protect code at rest

Control 9.2

Any developed application which requires roll out in production, need to be tested thoroughly for compliance as per stc Cyber Security Policies.

Threat modeling and risk assessment must be conducted during design to identify and address security risks.

Applications shall undergo static and dynamic security testing prior to production deployment, with all findings addressed.

Control 9.3
Approval from the **stc** Cyber Security team is required before any rollout to production. When an application has expired, it needs to be ensured that all related code with the expired application is removed from the production environment. Audit trail features in the Application and database systems shall always be kept enabled.

SUPPLIER RELATIONSHIP SECURITY CONTROLS

Control Type: Mandatory	**Reference ID:** ISMS-POL-11 Supplier Relationship Security Policy

Control Objective:
To ensure the protection of the organization's assets that is accessible by suppliers and to maintain an agreed level of information security and service delivery in line with supplier agreements.

Implementing Guidelines:
stc MS Vendors at the most basic level should have the following controls with reference to Supplier Relationship Security.

Control 10.1

- Information security requirements for mitigating the risks associated with suppliers' access to **stc**'s information assets must be agreed upon with the supplier and documented. Security controls compliant with the Standards must be implemented before permitting suppliers to access the **stc**'s information assets. The controls include processes and procedures to be implemented by **stc** and those that must be implemented by the supplier.
- Arrangements with suppliers that involve accessing, processing, storing, communicating, or managing **stc**'s information, information systems or information processing facilities must be based on a formal agreement containing necessary security requirements.

Control 10.2

The **stc** Cybersecurity team in coordination with the respective supplier management department shall monitor and review the Cybersecurity-related terms and conditions in agreements with suppliers. Non-security related items must be handled in accordance with Procurement Policies of **stc**. The processes must include:

- Reviewing service reports produced by the supplier.
- Enforcing Suppliers and MS vendors to conduct cyber security workshops and awareness for their teams on annual basis and provide evidence on their credentials.
- Enforce vendors to accept the installation of appropriate security software/agents on their team devices.
- Enforce orientation and awareness mandates for Vendors and their team to read and understand all cyber security policies, processes, and procedures.
- Ensuring the supplier maintains sufficient service capability, where applicable.

CYBERSECURITY INCIDENT MANAGEMENT CONTROLS

Control Type: Mandatory	**Reference ID:** ● ISMS-POL-12 Cybersecurity Incident Management Policy ● ISMS-PR01-p03 Non Conformance and Corrective Action Procedure ● ISMS-PR10-p01 Cyber Security Incident Management Procedure

Control Objective:

To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Implementing Guidelines:

stc MS Vendors at the most basic level should have the following controls with reference to Cybersecurity Incident Management.

Control 11.1

a) **stc** shall adopt an Information Security Incident Management framework by establishing Information security incidents management procedure which is inclusive of the following aspects:
   - Immediate notification of cyber security incidents.
   - Identification and response to various types of potential Cyber Security incidents.
   - Implementation of appropriate corrective action.
   - Provisioning of a formal report for critical incidents describing the incident, actions taken and recommended preventive measures.

b) The implementation of this policy shall establish the following mechanism:
   - Awareness of staff, contractors, and other users of Information Systems
   - Approved reporting channels for personnel to report Cyber Security incidents (actual or suspected breaches).
   - Adequate internal or external resources shall be made available to perform forensic investigations, if required
   - Appropriate Corrective / Preventive actions shall be identified to respond to the incident
   - Recommend proactive measures, to avoid similar incidents in the future based on lessons learned.

Control 11.2

Nonconformities may be identified from any source and the **stc** Cyber Security GM will encourage staff, users, customers and suppliers to propose ways in which they can be addressed.

Control 11.3

A Cyber Security event/incident may be detected by anybody in **stc**. Keeping the appropriate people informed is of paramount importance. For this purpose, all external parties and third-party users, wherever appropriate, should be made aware of the process of reporting such events / incidents and the following points need to be acted upon:

a) The employee / external party / third-party user, who notices the Cyber Security event / incident or malfunction, should report it as soon as possible to the **stc** Cyber Security team via Service desk.
b) Comprehensive contact information should be set out to ensure effective communication among responsible personnel. Updated contact information such as an office hour hotline and a non-office hour hotline, email address and mobile should be included where necessary.

Control 11.4

A Cyber Security weakness could be a bug or a weakness in the information system or service which if left unattended / unmanaged may result in Cyber Security events/incidents. For this purpose, the following need to be acted upon:

a) external party and third-party users shall report any observed or suspected Cyber Security weakness in their information systems or services to the **stc** Cyber Security team via the **stc** Service desk.
b) The Cyber Security team, in coordination with the **stc** IT GM, may take up appropriate action with the respective service provider/vendor as quickly as possible so as to prevent the occurrence of any security incidents due to such a security weakness in the system or service.

PASSWORD CONTROLS

Control Type: Mandatory	**Reference ID:** ISMS-POL-15 Password Policy

Control Objective:
Ensure to deploy complex passwords for accessing the information and information assets in the environment.

Implementing Guidelines:
stc MS Vendor at the most basic level should have the following configuration settings relate to password control.

Control 13.1
Systems shall be configured to ensure that the initial, temporary passwords for newly allocated accounts are changed at the first logon, and a record of the last five passwords for the account shall be maintained to prevent password reuse.

Control 13.2
First-time passwords should be forced to expire if the user does not access their account after a pre-defined period.

Control 13.3
If user credentials are stored in an application/ database, the data owner is responsible for implementing protection measures like encryption of the credential files/passwords. The respective department shall coordinate with the application vendor to ensure this aspect.

Control 13.4
Passwords should not be transmitted in clear text form over any kind of network.

Control 13.5
By default, all applications and systems should be configured to not display passwords on the screen while being keyed in.

Control 13.6
stc security team to provide user awareness training to all the users (including the third-party vendor employees, contract employees) to ensure password procedures and policies are followed by all the users.

Control 13.7
The Passwords must not be based on the company's name or geographic location.

Control 13.8
Password shall be protected by the Users and Users shall be responsible for the activities performed through their 'User ID'.

Control 13.9
Passwords should not be shared.

Control 13.10
Corporate Password shall never be used on an account over the internet which does not have a secure login or where the web browser address starts with 'http://' rather than 'https://'.

Control 13.11
Third-party vendors should comply with **stc** password policy. The complexity requirements should include a minimum of the following points:

a) Minimum password age should be set for one day.
b) Minimum password length should of 12 characters.
c) Records of the last 5 passwords (password history) should be maintained in order to prevent its reuse.
d) Password should contain a mix of alphabetic and non-alphabetic characters (number, punctuation or special characters) or a mix of at least two types of non-alphabetic characters.
e) The password shall be case sensitive and shall contain the combination of upper and lower case (e.g., a-z, A-Z).
f) Maximum password age for user accounts should be set for 90 days and administrator accounts for 90 days respectively. g) Account lockout threshold should be 5 successive invalid login attempts.
g) Account lockout duration and reset account lockout duration should be set for 0 minutes and 30 minutes respectively.

Control 13.12
The **stc** Cyber Security team should be informed in case it was identified or suspected that someone's password has been compromised.

Control 13.13
Password shall not be based on the following as mentioned below:

a) Months of the year, days of the week or any other aspect of the date (like date of birth, date of joining, etc.). b) Family names or initials.
h) Vehicle registration numbers.
i) Employee No. / Employee Id or designations.
j) Computer terms & names, commands, sites, companies, hardware, software.
k) Project or department name or references.
l) Company names, identifiers or references or Publicly known passwords (i.e. 123456, **stc**, **stc**1234, **stc**123, **stc**1234, admin, password, viva@1234, Viva@1234etc.).
m) Telephone numbers or similar all-numeric groups.
n) User ID, username, group ID or another system identifier.
o) All-number or all-alphabetic groups.

Control 13.14
Application developers must ensure that their programs contain the following password security precautions:

p) Should support authentication of individual users, not groups.
q) Should not store passwords in clear text or in an easily retrievable form.
r) Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
s) Should support TACACS+, Remote Authentication Dial-In User Service (RADIUS), Active Directory Services retrieval, wherever possible.

Control 13.15
Passwords should be memorized and never written down or recorded along with corresponding account information or usernames.

DOCUMENT CONTROL CONTROLS

Control Type: Mandatory	**Reference ID:** ISMS-PR02-p02 Document Control Procedure
Control Objective: Ensure that the required controls and processes are in place while creating, accessing, modifying, storing and disposing the ISMS artifacts.	
Implementing Guidelines: **stc** MS Vendors at the most basic level should have the following controls with reference to document control.	

Control 14.1

a) All contractors and third-party vendors must be aware of their responsibilities when writing, developing, or authorizing a document for **stc**.
b) This guideline clarifies the documentation requirements and underlines the compliance with which **stc** views the documentation and version control of the documents being written, developed, or authorized.
c) Users are expected to observe the arrangements set out in this guideline and procedure and to report any circumstances where they believe there is a breach in the control or usage of the documents appropriately.
d) Violation of the legal requirement for Data retention/Record retention may subject the individual to disciplinary action, as well as personal liability for civil and/or criminal sanctions by the courts or law enforcement agencies.

Control 14.2

a) All documents, which are initially prepared, should be considered as drafts.
b) On review of the draft document, it should be versioned and subsequently incremented for each review until approval.
c) A draft document becomes an approved document if it is approved by the appropriate authority.
d) Any major change in the document should be treated as a version change, otherwise it should be treated as a revision change.
e) By making a version/revision change, the earlier document should be marked as superseded.
f) Controlled copies should be destroyed when replaced with a new version/revision.
g) The changes should be incorporated in the electronic document and the entire document should be copied to the locations holding controlled copies.

CYBER SECURITY BUSINESS CONTINUITY MANAGEMENT CONTROLS

Control Type: Mandatory	**Reference ID:** ISMS-PR05-p01 Cyber Security Business Continuity Management Procedure

Control Objective:
To establish plans and procedures to be used in the event of an outage, which includes contingency plans, disaster recovery plans and procedures, and business continuity plan.

Implementing Guidelines:
stc MS Vendors at the most basic level should have the following controls with reference to cyber security business continuity management.

Control 15.1

a) Business continuity management should include controls to identify and reduce risks to the availability of critical services in addition to the general risk assessment process, limit the consequences of damaging incidents, and information required for business processes are readily available.
b) Business process owners should identify the key events that can cause disruption to their processes and document their potential adverse impact e.g. Impact categories – Financial impact, Health, safety, and environment quality impact, Reputational impact and Regulatory impact
c) The owner of the Business Continuity Plan should be responsible for coordinating updates to the plan, including documentation and procedural updates. This includes, but is not limited to:
   - Current location and contact information for parties relevant to the plan.
   - Procedures or processes necessary for the execution of the plan.
   - Third-party agreements, as applicable.
   - Asset inventories or requirements for the plan.
   - Training, awareness and education materials for participants.
   - Documentation on Cyber Security and controls requirements.

CHANGE MANAGEMENT CONTROLS

Control Type: Mandatory	**Reference ID:** ISMS-PR06-p01 Change Management Procedure

Control Objective:
To establish and sustain an effective and efficient change management system to control and manage all changes including emergency maintenance, documentation, security patches, relating to infrastructure and applications within the production environment and minimize the likelihood of disruption due to unauthorized alterations, and errors.

Implementing Guidelines:
stc MS Vendors at the most basic level should have the following controls with reference to change management procedures.

Control 16.1

a) Documentation for a change request shall be accompanied by detailed change requirements and appropriate procedures to carry out the change. It should also include detailed roll back procedures/plans, impact in case the change fails and / or desired result is not achieved.
b) Change management process shall facilitate communication and notification of all changes to the affected internal and external stakeholders within **stc**.
c) Adequate segregation of duties shall be maintained to ensure that changes to production systems cannot be implemented single handedly.
d) Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimize the impact on the relevant business process/operations.
e) User acceptance testing shall be conducted to ensure that changes implemented have met the anticipated objectives defined in the Change Request.

SYSTEM UPDATE CONTROLS

Control Type: Mandatory	**Reference ID:** ISMS-PR07-p01 System Update Procedure
Control Objective: To provide advice on patching IT systems so as to better secure them from attack and vulnerability assessment pertaining to **stc** Network.	
Implementing Guidelines: **stc** MS Vendors at the most basic level should have the following controls with reference to system update procedures.	
Control 17.1 a) **stc** shall establish a process to identify newly discovered security vulnerabilities through the following means: ● Subscription to advisory and alert lists which notify any new software updates or patches that are released. ● Direct notification from vendors and software providers. ● Vulnerability assessment reports from the Cyber Security team. b) All IT and Network systems should have latest updates / patches / service packs / hotfixes installed as per planned schedules. c) There should be a mechanism to test the updates / patches / service packs/ hot fixes for all business-critical systems and application in a test environment before they are applied on live systems. d) To ensure that patching is done regularly in a controlled and predictable manner a patch schedule should be created. e) Patch deployment shall be carried out through the Change Management process as applicable. f) Downtime estimation, if any, for the deployment of patches shall be done for production environments. Arrangements should be made to inform the users in advance about downtime or downtime can be planned off business hours. g) Rollback mechanisms shall be in place in case of unexpected issues, so that the system can be brought to the previous state. h) Patches to remediate zero-day vulnerabilities shall be deployed as soon as the patch is released by the vendor and in accordance with the stipulated timelines. i) If patches are not available, vendors must implement compensatory controls / workarounds to mitigate the risk within the agreed SLA. j) Teams applying patches are required to compile, report and maintain reporting metrics that record percentages of systems that are effectively patched summarizing the outcome of each patching cycle. k) Logs must document patches and updates that have been installed on each laptop, desktop and server including patch details, date of installation, and name of the assigned person installing the patch.	

INFORMATION TRANSFER CONTROLS

Control Type: Mandatory	**Reference ID:** ISMS-PR08-p01 Information Transfer Procedure
Control Objective: Adequately protect the information for legal reasons such as confidentiality or data protection, and to maintain the trust of our service users and partners.	
Implementing Guidelines: **stc** MS Vendors at the most basic level should have the following controls with reference to information transfer procedures.	
Control 18.1 ● The email system is **stc**'s property and all copies of messages created, sent, received or stored on the system are the property of **stc**. ● **stc** maintains the right to review, audit, intercept, access, monitor, delete and disclose all messages created, received, sent or stored on the email system upon approval from the Management Committee. ● **stc** provides electronic information and communications systems to facilitate the **stc**'s business needs and interests. ● All access to electronic messages shall be limited to properly authorized personnel. ● **stc** information resources shall not be used to transmit or receive statements that contain any material that is offensive, defamatory, or threatening to others.	

- Any statements or comments made via E-Mail that shall in any way be construed as an action of **stc** shall bear the following disclaimer:
  - This email may contain information pertaining to **stc**, due to the personal business contract of the sender with **stc**. **stc** accepts no liability for the content of this email, or for the consequences of any actions taken on the basis of the information provided, unless that information is subsequently confirmed in writing by **stc**.
- Email Id created for Vendor / Third Party / Managed Services staff shall be disabled / removed upon engagement / contractual agreement completion with **stc**.
- Each user shall take precautions to prevent unauthorized use of the E-Mail accounts. Users are personally responsible for all emails from their account. Forging of the header information in E-Mail (including source address, a destination address, and timestamps) shall not be permitted.
- **stc** systems shall not be used to transmit or receive trade secrets, copyrighted materials, or proprietary or confidential information.
- Any information regarded as confidential including legal or contractual agreements, technical information related to **stc**'s operations or security etc. shall not be communicated through e-Mail without adequate measures to protect the attached information from unauthorized access.
- **stc** reserves the right to monitor or restrict web access of its Emails. Users have a responsibility to ensure that they do not access **stc** emails from public systems like those in internet cafes. In case of any extreme need to access **stc** email from a public computer, the user needs to ensure that all temporary/local copies of the emails and attachments are removed from the system and the user credentials are not stored in the system.

Control 18.2
- The default mailbox size for **stc** employees is 1.1 GB and to that of any contractor it is 110 MB. However, users can request additional mailbox sizes with a valid business reason and appropriate approval.
- Content filtering solution shall be configured to block suspicious messages in emails.

Control 18.3
- Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions.
- Employees, contractors, clients, vendors, consultants shall not use any other type of connections when the system / device is connected to the **stc** Corporate network.

Control 18.4
- All content downloaded from the Internet shall be scanned at the gateway and at the clients to ensure that the same is free from any malicious code such as viruses, Trojan horses or worms.
- Users are not allowed to download or upload any software from/to the internet without prior approval.
- The Internet service shall be used to enhance the professional contribution of users to the company. All users shall also ensure that they use the Internet services in an ethical and lawful manner to avoid litigation for **stc**.

Control 18.5
Users should be aware that **stc** shall accept no liability for their exposure to offensive material that they may access via the Internet. Users should not access websites that are blocked by the Government and Users shall also not visit unofficial sites or suspicious websites. The following is a list of illustrative examples of unacceptable use of Internet services:
- Transmitting any content that is offensive, harassing or fraudulent, breaks the law or discredits the organization / governing authorities.
- Conducting personal business using company resources.
- Downloading of unlicensed software.
- Sending threatening messages or files.
- Sending sexually or racially harassing messages or files.
- Sending files containing computer viruses or other malicious code.
- Attempting to access systems without proper authorizations.
- Sending or posting confidential information to unauthorized persons.
- Posting configuration Information or details of potential vulnerabilities in **stc** IT infrastructure on public domains.
- Accessing/downloading pornographic, racist or illegal sites, pictures, songs, jokes, animations, graphics, movies or any other material.
- Using the internet for accessing sites promoting gambling, personal commercial benefits or money laundering.
- Establish Internet or other external network connections that could allow non- **stc** users to gain access into **stc**'s Systems and Applications.
- Intentionally interfere with the normal operation of an internet gateway.
- Inbound and outbound unsecured Terminal Service connections through the internet shall not be permitted. ● Internal relay chat & P2P services are prohibited.

CYBER SECURITY VENDOR GOVERNANCE CONTROLS

Control Type: Mandatory	**Reference ID:** ISMS-PR09-p01 Cyber Security Vendor Governance Procedure
Control Objective: To set out the basic rules for managing the security over third parties (i.e., suppliers, vendors etc) who maintain direct or indirect access to **stc** systems and data.	
Implementing Guidelines: **stc** MS Vendors at the most basic level should have the following controls with reference to Cyber Security Vendor Governance.	

Control 19.1
MS Vendors should use **stc** baseline controls and Assessment Checklist to develop a viable security assessment plan for producing and compiling the information necessary to determine the effectiveness of the security controls employed in the information system. In developing effective security assessment plans, MS Vendors should take into consideration existing information about the security controls to be assessed.

Control 19.2
The information produced during security control assessments can be used by the MS Vendor to:

a) Identify information system weaknesses and deficiencies
b) Confirm that identified weaknesses and deficiencies in the information system have been addressed.c) Support budgetary decisions and capital investment.

Control 19.3
Managed Service Vendors Contractually and operationally commit to meeting **stc** commercial, security and any regulatory compliance obligations. The following requirements must be included in third party agreements:

a) External parties are covered by a non-disclosure agreement that explicitly states that persons with access to **stc** facilities or proprietary information are not to disseminate any information about **stc**, its capabilities or activities without written authorization from **stc**.
b) The obligation of the third party to notify **stc** in cases of security incidents occurring within the third party, which may affect **stc** (e.g. third-party virus outbreak, successful third party network compromise etc).
c) The obligation of the third party to maintain confidentiality integrity and availability of **stc** information.
d) The possibility of renegotiating or terminating the contract if the terms and conditions are not satisfied, for example an undisclosed security incident or third party failing to meet agreed service levels.
e) Sub-contracting issues in case the third parties make use of other suppliers for the delivery of the services and these suppliers maintain direct or indirect access to **stc**'s data. The third party must commit that any suppliers meet **stc** security and regulatory compliance obligations.
f) Controls must be in place to ensure the security of remote connections between the parties. The third party must utilize the existing **stc** security infrastructure and take responsibility for the maintenance of the respective security controls that have been established by **stc**.
g) Ownership of licensing and intellectual property, including escrow agreements must be clearly defined.
h) To the extent possible, a "right to Audit" clause ensuring that management and/or an authorized representative may physically and or logically evaluate a third party's control environment.
i) The type, volume and frequency of any files and/or reports that will be exchanged between the two parties.
j) The business continuity and disaster recovery arrangements for the resumption of the third-party services in case of service interruption or data loss/destruction.

INFORMATION BACKUP CONTROLS

Control Type: Mandatory	**Reference ID:** ISMS-PR-12-p01 Backup Procedure
Control Objective: Ensure to conduct backups of user-level information, Corporate data encompassing emails, transactions, customer data, Business plans/strategy and system level information contained in the information system.	
Implementing Guidelines: **stc** MS Vendor at the most basic level should have the following controls in relation to Information system backup.	
Control 20.1 Identify, document and back up critical organization data including but not limited to the following: a) User level data: System/applications users, employee details etc. b) System level data: Operating system, application software, licenses etc. c) Business data: Customer data, Business Plans, emails, Product info etc.	

Control 20.2
Define and document Backup Strategy stating the following:

a) Types of data to be backed up e.g. corporate data, user or system level etc.
b) Types of backup methods to be used e.g. weekly and monthly full backup; differential and incremental backup on weekdays. Refer to the table below for the backup method to invoke based on various business needs:

Backup Invocation	Need
Request for Backup	If there is a business need to backup any information, a request must be initiated; and this procedure will be triggered.
Emergency Backup Request / Disaster Response	In the event of an urgent change, disaster an emergency backup request shall be initiated; and this procedure will be triggered.
Conditional Backup Request (Change Request / Patch Implementation)	Ensuring that the backup and restoration procedure is properly implemented.
Periodic Backup Plan	If there is a periodic backup request, this procedure shall be invoked.
Availability Management for Backups	In the event of a disaster, an emergency backup availability will be initiated; and this procedure will be triggered.

a) Retention period of back up data. Refer to the table below for the **Stc** backup retention policy:

System	Type of Backup	Frequency	Owner	Retention	No of Copies	Onsite	Offsite
All Systems	Database	Incremental Daily	Application Manger	1 Month	2	Yes	Yes
		Full Weekly	Application Manger	3 Months	2	Yes	Yes
	File System	Full Monthly	Application Manger	6 Months	1	Yes	No
		Incremental Daily	Application Manger	1 Month	1	Yes	No
	CDRS Files	Incremental Daily	Application Manger	Infinity	2	Yes	Yes
	Speech Log Files	Incremental Daily	Application Manger	Infinity	2	Yes	Yes
	Exchange	Incremental Daily	Application Manger	3 Months	2	Yes	Yes
		Full Monthly	Application Manger	Infinity	2	Yes	Yes

b) Security of backup data e.g. encryption, storing offsite, test recovery etc.
c) Requirements of backup to tapes, disks or combination of both.

Control 20.3
Conduct backup as per defined backup strategy.

Control 20.4
Store backups in secure onsite locations e.g. if backup tapes are used then keep the tapes in fire- proof vaults.

Control 20.5
Save a second copy of backup in a remote location either electronically or by physical shipment of storage media.

Control 20.6
Use digital signatures and cryptographic hashes in order to protect the integrity of information system backups.

Control 20.7
Ensure backup availability for Business Continuity by testing restoration of backed up data using a sampling method.

INFORMATION CLASSIFICATION CONTROLS

Control Type: Mandatory	**Reference ID:** ISMS-PR12-p03 Information Classification Procedure
Control Objective: Establishing a framework for classifying **stc** data/information based on its level of sensitivity, value and criticality to the company.	
Implementing Guidelines: **stc** MS Vendor at the most basic level should have the following controls in relation to Information classification.	

Control 21.1
Information classification in **stc** is dependent on confidentiality, integrity or availability of information. The table below defines the Information Classification levels:

Level	Description
Public	This classification applies to Information that is available to the general public and intended for distribution outside the organization. This Information may be freely disseminated without potential harm. Although there are no restrictions on disclosure to protect public data (because the Information is provided for broad viewing access), sufficient protection must be applied to prevent unauthorized modification of such Information.
Internal use only	within the section of the organization. Unauthorized disclosures, modification or destruction of this data is not expected to seriously or adversely impact **stc**, its employees, or stakeholders. This classification applies to the Information that is considered private i.e. can be accessed only by a limited number of personnel is included in this classification.
Confidential	This classification applies to the Information that is considered private i.e. can be accessed only by a limited number of personnel is included in this classification. Unauthorized disclosure could adversely impact the organization, its employees and stakeholders. Information assets for which there are legal requirements prohibiting or imposing financial penalties for unauthorized disclosure. Information covered by regulatory and state law or legislation, Risk registers, Audit reports and finance information are in this class.
Top Confidential	This classification applies to highly sensitive information that, if disclosed, could cause severe damage to stc's operations, reputation, competitive position, or result in significant legal or regulatory consequences. Access is strictly limited to individuals with explicit authorization on a need-to-know basis. Examples include executive strategic plans, security architecture, credentials to critical systems, private keys, and national-level agreements or data.

Control 21.2
The following table defines Information Security Standards required safeguards for protecting Information based on their classification. In addition to the following Information security.

standards, any information covered by state laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts.

Security Control Category	Information Classification - Public	Information Classification - Company Restricted	Information Classification - Confidential
Access Controls	No restriction for viewing Authorization by Information Owner or designee required for Modification. Supervisor approval also required if not a self-service function	Viewing and modification restricted to authorized individuals as needed for business-related roles Information Owner or designee grants permission for access, plus approval from supervisor Authentication and authorization required for access.	Viewing and modification restricted to authorized individuals as needed for business-related roles Information Owner or designee grants permission for access, plus approval from supervisor Authentication and authorization required for access Confidentiality agreement required

Copying/Printing (applies to both paper and electronic forms)	No restrictions	Information should only be printed when there is a legitimate need Copies must be limited to individuals with a need to know Information should not be left unattended on a printer	Information should only be printed when there is a legitimate need Copies must be limited to individuals authorized to access the Information and have signed a confidentiality agreement Information should not be left unattended on a printer Copies must be labeled «Confidential»

Network Security	May reside on a public network Protection with a firewall recommended IDS/IPS protection recommended Protection only with router ACLs acceptable	Protection with a network firewall required IDS/IPS protection required Protection with router ACLs optional Servers hosting the data should not be visible to entire Internet May be in a shared network server subnet with a common firewall ruleset for the set of servers	Protection with a network firewall using «default deny» ruleset required IDS/IPS protection required Protection with router ACLs optional Servers hosting the data cannot be visible to the entire Internet, nor to unprotected subnets like the residence halls and guest wireless networks to the system The firewall ruleset should be reviewed periodically by an external auditor
System Security	Must follow general leading practices for system management and security (**stc** Minimum Security Baselines) Host-based software firewall recommended	Must follow **stc**- specific and OS specific best practices for system management and security Host-based software firewall required Host-based software IDS/IPS recommended	Must follow **stc**- specific and OS specific best practices for system management and security Host-based software firewall required Host-based software IDS/IPS recommended
Virtual Environments	May be hosted in a virtual server environment All other security controls apply to both the host and the guest virtual machines	May be hosted in a virtual server environment All other security controls apply to both the host and the guest virtual machines Should not share the same virtual host environment with guest virtual servers of other security classifications	May be hosted in a virtual server environment All other security controls apply to both the host and the guest virtual machines Cannot share the same virtual host environment with guest virtual servers of other security classifications
Physical Security	System must be locked or logged out when unattended Host-based software firewall recommended	System must be locked or logged out when unattended Hosted in a secure location required; a Secure Data Center is recommended	System must be locked or logged out when unattended Hosted in a Secure Data Center required Physical access must be monitored, logged, and limited to authorized individuals 24x7
Remote Access to systems hosting the data	No restrictions	Access restricted to local network or general **stc** Virtual Private Network (VPN) service Remote access by third party for technical support limited to authenticated, temporary access via direct dial-in modem or secure protocols over the Internet	Restricted to local network or secure VPN group Unsupervised remote access by third party for technical support not allowed Twofactor authentication recommended

Information Storage	Storage on a secure server recommended Storage in a secure Data Center recommended	Storage on a secure server recommended Storage in a secure Data Center recommended Should not store on an individual›s workstation or a mobile device	Storage on a secure server required Storage in Secure Data Center required Should not store on an individual workstation or mobile device (e.g., a laptop computer); if stored on a workstation or mobile device, must use whole-disk encryption Encryption on backup media required AES Encryption required with 192- bit or longer key Paper/hard copy: do not leave unattended where others may see it; store in a secure location
Transmission	No restrictions	No requirements	Encryption required (for example, via SSL or secure file transfer protocols). Cannot transmit via e-mail unless encrypted and secured with a digital signature
Backup/Disaster Recovery	Backups required; daily backups recommended	Daily backups required. Offsite storage recommended	Daily backups required. Off-site storage in a secure location required
Training	General security awareness training recommended. System administration training recommended	General security awareness training required. System administration training required. Information security training required	General security awareness training required. System administration training required. System administrators hired after Sept. 1, 2008, must pass a criminal background check Information security training required. Applicable policy and regulation training required
Audit Schedule	As needed	As needed	Annual

Control 21.3
To ensure that the correct controls are applied to the information assets of **stc**, a system of protective marking will be used so that all third parties, where applicable, are aware of how that information must be managed.
Control 21.4
Strict controls are placed on the use of removable media such as CDs, DVDs, tapes, external hard drives and USB memory sticks within **stc**. Legitimate use of these Devices should be authorized before use.

APPENDIX - 1

End User Security - Staff should follow clear desk and clear screen requirements at all times.

CLEAR DESK

The clear desk as the name suggests is for physical information security either on the individuals' desk or on the printer or any other unattended location. Below points are guidelines on achieving the same:

- Confidential information must be locked away when not in use and never left unattended.
- Classified information must be removed from the vicinity of the printers and should not be left in the collection tray of the printer.
- It is always a good practice to switch off printers outside of normal working hours.
- An easy way to comply with the clear desk procedure is to work with electronic documents whenever possible asking a question "do I need to print this?"
- Taking electronic scanned copies rather hard copy paper and saving it to an appropriate secure network drive or email address reduces the risk of unattended data or information falling into unauthorized hands.
- Ensure hardcopy documents are disposed of securely.
- Never put documents containing personal or corporate sensitive information in the general waste bins nor leave it unattended on the desk.

- Where appropriate, store paper and computer media in suitable containers when not in use, even during working hours.
- Lock away classified material when not needed, especially when the office is unoccupied.
- Use the confidential waste bag or confidential boxes secured with a lock and key or shred documents as appropriate.
- All Portable Computing & Data Storage Devices (PCDs) such as USB data sticks, mobile phones and laptops should be kept securely at the end of the working day.
- Protect incoming and outgoing mail points and unattended fax machines.
- ID cards that give access to printing should not be left unattended and must be carried by staff at all times.

CLEAR SCREEN

- Always Lock/Log-off devices such as computer terminals or printers when unattended.
- If using a shared workstation log off rather than locking it.
- Pressing CTRL+ALT+DEL is straightforward and simple to lock the computer. However, a windows key combination is even simpler. Press windows key + L and your computer will lock automatically. The windows key can usually be found in the bottom left of the keyboard and looks like a flag/window.
- Always be aware of the position of the screen on your workstation. Wherever possible, ensure that it cannot be seen by unauthorized people while in use.
- Use a screen saver with a password, which shall be activated after 3 minutes of inactivity/idle time.
- The monitors should also be turned off at the end of the working day.