stratagile

(re)defining digital marketing

Information Security Policy

ISP/2013/10/10/D05

Table of Contents

1. Policy

It is the policy of StratAgile that information, as defined hereinafter, in all its forms - written, spoken, recorded electronically or printed - will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

All policies and procedures must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented. All the documentation, which may be in electronic form, must be retained for at least 5 (five) years after initial creation, or, pertaining to policies and procedures, after changes are made. All documentation must be periodically reviewed for appropriateness and currency, a period of time to be determined by each entity within StratAgile.

At each entity and/or department level, additional policies, standards and procedures will be developed detailing the implementation of this policy and set of standards, and addressing any additional information systems functionality in such entity and/or department. All departmental policies must be consistent with this policy. All systems implemented after the effective date of these policies are expected to comply with the provisions of this policy where possible. Existing systems are expected to be brought into compliance where possible and as soon as practical.

2. Scope

The scope of information security includes the protection of the confidentiality, integrity and availability of information.

The framework for managing information security in this policy applies to all StratAgile entities and workers, and other Involved Persons and all Involved Systems throughout StratAgile as defined below in INFORMATION SECURITY DEFINITIONS.

This policy and all standards apply to all protected health information and other classes of protected information in any form as defined below in INFORMATION CLASSIFICATION.

3. Risk management

A detailed analysis of all StratAgile information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats – internal

or external, natural or manmade, electronic and non-electronic-- that affect the ability to manage the information resource. The analysis will also document the existing vulnerabilities within each entity which potentially expose the information resource to the threats. Finally, the analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk analysis will be determined at the entity level.

Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

4. Information security definitions

Affiliated Covered Entities: Legally separate, but affiliated, covered entities which choose to designate themselves as a single covered entity.

Availability: Data or information is accessible and usable upon demand by an authorized person.

Confidentiality: Data or information is not made available or disclosed to unauthorized persons or processes.

Integrity: Data or information has not been altered or destroyed in an unauthorized manner.

Involved Persons: Every worker at StratAgile, no matter what their status. This includes employees, contractors, consultants, temporaries, interns, etc.

Involved Systems: All computer equipment and network systems that are operated within the StratAgile environment. This includes all platforms (operating systems), all computer sizes BYOD's, (personal digital assistants, desktops, mainframes, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.

Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

5. Information security responsibilities

Information Security Officer: The Information Security Officer (ISO) for each entity is responsible for working with user management, owners, custodians, and users to develop and implement prudent security policies, procedures, and controls, subject to the approval of StratAgile. Specific responsibilities include:

- Ensuring security policies, procedures, and standards are in place and adhered to by entity.
- Providing basic security support for all systems and users.
- Advising owners in the identification and classification of computer resources. See Section VI Information Classification.
- Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.
- Educating custodian and user management with comprehensive information about security controls affecting system users and application systems.
- Providing ongoing employee security education.
- Performing security audits.
- Reporting regularly to the StratAgile Oversight Committee on entity's status with regard to information security.

Information Owner: The owner of a collection of information is usually the manager responsible for the creation of that information or the primary user of that information. This role often corresponds with the management of an organizational unit. In this context, ownership does not signify proprietary interest, and ownership may be shared. The owner may delegate ownership responsibilities to another individual by completing the StratAgile Information Owner Delegation Form. The owner of information has the responsibility for:

- Knowing the information for which she/he is responsible.
- Determining a data retention period for the information, relying on advice from the Legal Department.
- Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created within the unit.
- Authorizing access and assigning custodianship.
- Specifying controls and communicating the control requirements to the custodian and users of the information.
- Reporting promptly to the ISO the loss or misuse StratAgile information.
- Initiating corrective actions when problems are identified.
- Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.

- Following existing approval processes within the respective organizational unit for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.
- Custodian: The custodian of information is generally responsible for the processing and storage of the information. The custodian is responsible for the administration of controls as specified by the owner. Responsibilities may include:
- Providing and/or recommending physical safeguards.
- Providing and/or recommending procedural safeguards.
- Administering access to information.
- Releasing information as authorized by the Information Owner and/or the Information Privacy/ Security Officer for use and disclosure using procedures that protect the privacy of the information.
- Evaluating the cost effectiveness of controls.
- Maintaining information security policies, procedures and standards as appropriate and in consultation with the ISO.Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
- Reporting promptly to the ISO the loss or misuse StratAgile information.
- Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

User Management: StratAgile management who supervise users as defined below. User management is responsible for overseeing their employees' use of information, including:

- Reviewing and approving all requests for their employee's access authorizations.
- Initiating security change requests to keep employees' security record current with their positions and job functions.
- Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures.
- Revoking physical access to terminated employees, i.e., confiscating keys, changing combination locks, etc.
- Providing employees with the opportunity for training needed to properly use the computer systems.
- Initiating corrective actions when problems are identified.
- Following existing approval processes within their respective organization for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

User: The user is any person who has been authorized to read, enter, or update information. A user of information is expected to:

- Access information only in support of their authorized job responsibilities.
- Comply with Information Security Policies and Standards and with all controls established by the owner and custodian.

- Refer all disclosures outside of StratAgile and (within StratAgile
- Keep personal authentication devices (e.g. passwords, Secure Cards, PINs, etc.) confidential.
- Initiate corrective actions when problems are identified.

6. Information classification

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format. The following levels are to be used when classifying information:

Confidential information

- Confidential Information is very important and highly sensitive material. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access.
- Examples of Confidential Information may include: personal information, key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.
- Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for StratAgile, its customers, or its business partners. Decisions about the provision of access to this information must always be cleared through the information owner.

Internal Information

- Internal Information is intended for unrestricted use within StratAgile, and in some cases within affiliated organizations such as StratAgile business partners. This type of information is already widely-distributed within StratAgile, or it could be so distributed within the organization without advance permission from the information owner.
- Examples of Internal Information may include: personal directories, internal policies and procedures, most internal electronic mail messages.
- Any information not explicitly Confidential or Public will, by default, be classified as Internal Information.
- Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

Public Information

- Public Information has been specifically approved for public release by a designated authority within each entity of StratAgile. Examples of Public Information may include marketing brochures and material posted to StratAgile entity internet web pages.
- This information may be disclosed outside of StratAgile.

7. Computer and information control

All involved systems and information are assets of StratAgile and are expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

Ownership of Software: All computer software developed by StratAgile employees or contract personnel on behalf of StratAgile or licensed for StratAgile use is the property of StratAgile and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.

Installed Software: All software packages that reside on computers and networks within StratAgile must comply with applicable licensing agreements and restrictions and must comply with StratAgile acquisition of software policies.

Virus Protection: Virus checking systems approved by the Information Security Officer and Information Services must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus checking systems.

Access Controls: Physical and electronic access to Confidential and Internal information and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures will be instituted as recommended by the Information Security Officer and approved by StratAgile. Mechanisms to control access to Confidential and Internal information include (but are not limited to) the following methods:

- ***Authorization***: Access will be granted on a “need to know” basis and must be authorized by the immediate supervisor and application owner. Any of the following methods are acceptable for providing access under this policy:
- ***Context-based access:*** Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The “external” factors might include time of day, location of the user, strength of user authentication, etc.
- ***Role-based access:*** An alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way

that maps more naturally to an organization's structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.

- ***User-based access:*** A security mechanism used to grant users of a system access based upon the identity of the user.

Identification/Authentication: Unique user identification (user id) and authentication is required for all systems that maintain or access Confidential and/or Internal Information. Users will be held accountable for all actions performed on the system with their user id.

- At least one of the following authentication methods is be implemented:
  - strictly controlled passwords
  - biometric identification, and/or
  - tokens in conjunction with a PIN.
- The user must secure his/her authentication control (e.g. password, token) such that it is known only to that user and possibly a designated security manager.
- An automatic timeout re-authentication must be required after a certain period of no activity (maximum 15 minutes).
- The user must log off or secure the system when leaving it.

Data Integrity: Confidential, and Internal Information has not been altered or destroyed in an unauthorized manner. Following methods that support data integrity are to be used:

- Transaction audit
- Disk redundancy (RAID)
- ECC (Error Correcting Memory)
- Checksums (file integrity)
- Encryption of data in storage
- Digital signatures

Transmission Security: Technical security mechanisms must be put in place to guard against unauthorized access to data that is transmitted over a communications network, including wireless networks. The following features must be implemented:

- integrity controls and
- encryption, where deemed appropriate

Remote Access: Access to StratAgile network from outside will be granted using StratAgile approved devices and pathways on an individual user and application basis. All other network access options are strictly prohibited. Further, Confidential and/or Internal Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within the StratAgile network.

Physical Access: Access to areas in which information processing is carried out must be restricted to only appropriately authorized individuals. The following physical controls must be in place:

- File servers containing Confidential and/or Internal Information must be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.
- Workstations or personal computers (PC) must be secured against use by unauthorized individuals. Local procedures and standards must be developed on secure and appropriate workstation use and physical safeguards which must include procedures that will:
    - Position workstations to minimize unauthorized viewing of protected health information.
    - Grant workstation access only to those who need it in order to perform their job function.
    - Establish workstation location criteria to eliminate or minimize the possibility of unauthorized access to protected health information.
    - Employ physical safeguards as determined by risk analysis, such as locating workstations in controlled access areas or installing covers or enclosures to preclude passerby access to Confidential Information.
    - Use automatic screen savers with passwords to protect unattended machines.
- Facility access controls must be implemented to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. Local policies and procedures must be developed to address the following facility access control requirements:
    - Contingency Operations – Documented procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
    - Facility Security Plan – Documented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
    - Access Control and Validation – Documented procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
    - Maintenance records – Documented policies and procedures to document repairs and modifications to the physical components of the facility which are related to security (for example, hardware, walls, doors, and locks).

Emergency Access: Each entity is required to establish a mechanism to provide emergency access to systems and applications in the event that the assigned

custodian or owner is unavailable during an emergency. Procedures must be documented to address:

- Authorization
- Implementation
- Revocation

Equipment and Media Controls: The disposal of information must ensure the continued protection of Confidential and Internal Information. Each entity must develop and implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain confidential Information into and out of a facility, and the movement of these items within the facility. The following specification must be addressed:

- Information Disposal / Media Re-Use of:
    - Hard copy (paper and microfilm/fiche)
    - Magnetic media (floppy disks, hard drives, zip disks, etc.)
    - CD ROM Disks
- Accountability: Each entity must maintain a record of the movements of hardware and electronic media and any person responsible therefore.
- Data backup and Storage: When needed, create a retrievable, exact copy of electronic information before movement of equipment.

Other Media Controls:
Confidential Information stored on external media (diskettes, CD-ROMs, portable storage, memory sticks, etc.) must be protected from theft and unauthorized access. Such media must be appropriately labeled so as to identify it as Confidential Information. Further, external media containing confidential Information must never be left unattended in unsecured areas.

Confidential Information must never be stored on mobile computing devices (laptops, personal digital assistants/Tablets (PDA), smartphones, tablet PC's, etc.) unless the devices have the following minimum security requirements implemented:

- Power-on passwords
- Auto logoff or screen saver with password
- Encryption of stored data or other acceptable safeguards approved by Information Security Officer
- Further, mobile computing devices must never be left unattended in unsecured areas.

If Confidential Information is stored on external medium or mobile computing devices and there is a breach of confidentiality as a result, then the owner of the medium/device will be held personally accountable and is subject to the terms and conditions of StratAgile Information Security Policies and Confidentiality Statement signed as a condition of employment or affiliation with StratAgile.

Data Transfer/Printing:

Electronic Mass Data Transfers: Downloading and uploading Confidential, and Internal Information between systems must be strictly controlled. Requests for mass download of, or individual requests for, information for any purposes must be approved through the Internal Review Board (IRB). All other mass downloads of information must be approved by the Application Owner and include only the minimum amount of information necessary to fulfill the request. Applicable Business Associate Agreements must be in place when transferring CI to external entities

Other Electronic Data Transfers and Printing: Confidential and Internal Information must be stored in a manner inaccessible to unauthorized individuals. Confidential information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise.CI that is downloaded for educational purposes where possible should be de-identified before use.

Oral Communications:

StratAgile staff should be aware of their surroundings when discussing Confidential Information. This includes the use of cellular telephones in public areas. StratAgile staff should not discuss Confidential Information in public areas if the information can be overheard. Caution should be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairways, cafeterias, restaurants, or on public transportation.

Audit Controls: Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use CI must be implemented. Further, procedures must be implemented to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. These reviews must be documented and maintained for five (5) years.

Evaluation: StratAgile requires that periodic technical and non-technical evaluations be performed in response to environmental or operational changes affecting the security of electronic information to ensure its continued protection.

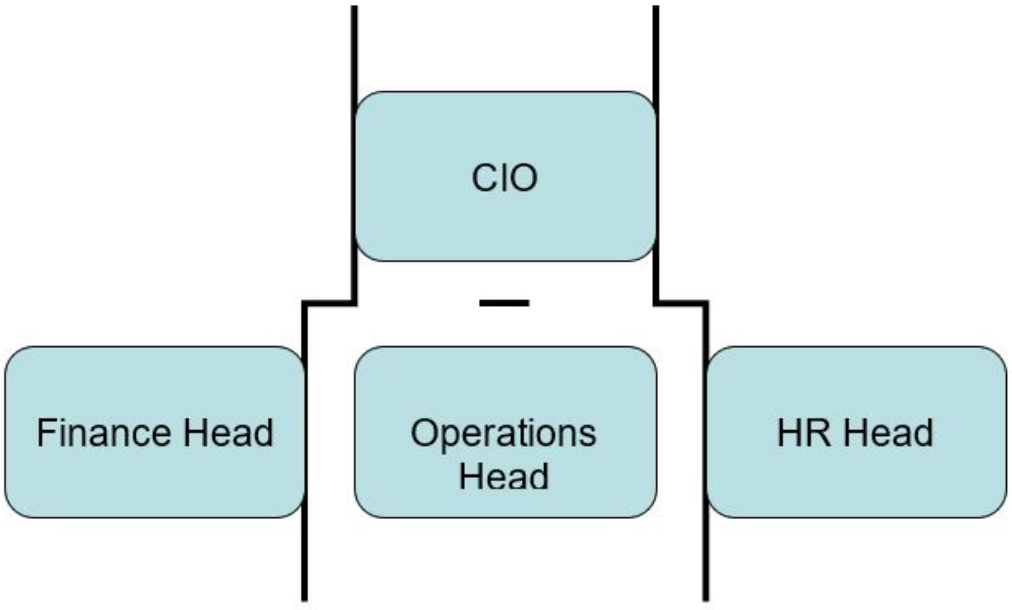
Contingency Plan: Controls must ensure that StratAgile can recover from any damage to computer equipment or files within a reasonable period of time. Each entity is required to develop and maintain a plan for responding to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain Confidential, or Internal Information. This will include developing policies and procedures to address the following:

- Data Backup Plan:
    - A data backup plan must be documented and routinely updated to create and maintain, for a specific period of time, retrievable exact copies of information.

    - Backup data must be stored in an off-site location and protected from physical damage.
    - Backup data must be afforded the same level of protection as the original data.
- Disaster Recovery Plan: A disaster recovery plan must be developed and documented which contains a process enabling the entity to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.
- Emergency Mode Operation Plan: A plan must be developed and documented which contains a process enabling the entity to continue to operate in the event of fire, vandalism, natural disaster, or system failure.
- Testing and Revision Procedures: Procedures should be developed and documented requiring periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.
- Applications and Data Criticality Analysis: The criticality of specific applications and data in support of other contingency plan components must be assessed and documented.

8. Information security program team structure

Following is the information security program team structure within StratAgile



The team comprises of CIO or CIO designate along with Finance, Operations and HR. CIO is responsible for the review and maintenance of the Information security policy. The review team will meet once in a quarter to assess any changes needed for the overall policy.

9. Internet, e-mail, and computer user policy

The use of StratAgile (Company) automation systems, including computers, fax machines, and all forms of Internet/intranet access, is for company business and for authorized purposes only. Brief and occasional personal use of the electronic mail system or the Internet is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense or harm to the Company or otherwise violate this policy.

Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. Electronic communication should not be used to solicit or sell products or services that are unrelated to the Company's business; distract, intimidate, or harass coworkers or third parties; or disrupt the workplace.

Use of Company computers, networks, and Internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:

- Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate Company purposes;
- Engaging in private or personal business activities, including excessive use of instant messaging and chat rooms
- Accessing networks, servers, drives, folders, or files to which the employee has not been granted access or authorization from someone with the right to make such a grant;
- Making unauthorized copies of Company files or other Company data;
- Destroying, deleting, erasing, or concealing Company files or other Company data, or otherwise making such files or data unavailable or inaccessible to the Company or to other authorized users of Company systems;
- Misrepresenting oneself or the Company;
- Violating the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way;
- Engaging in unlawful or malicious activities;
- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the Company's networks or systems or those of any other individual or entity;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- Sending, receiving, or accessing pornographic materials;
- Becoming involved in partisan politics;

- Causing congestion, disruption, disablement, alteration, or impairment of Company networks or systems;
- Maintaining, organizing, or participating in non-work-related Web logs ("blogs"), Web journals, "chat rooms", or private/personal/instant messaging;
- Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned, if you leave such computer or system unattended;
- Using recreational games; and/or
- Defeating or attempting to defeat security restrictions on company systems and applications.

Using Company automation systems to access, create, view, transmit, or receive racist, sexist, threatening, or otherwise objectionable or illegal material, defined as any visual, textual, or auditory entity, file, or data, is strictly prohibited. Such material violates the Company anti-harassment policies and subjects the responsible employee to disciplinary action. The Company's electronic mail system, Internet access, and computer systems must not be used to harm others or to violate the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way. Use of company resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution. The Company will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities, e-mail use, and/or computer use.

Unless specifically granted in this policy, any non-business use of the Company's automation systems is expressly forbidden.

If you violate these policies, you could be subject to disciplinary action, up to and including dismissal.

Ownership and access of electronic mail, internet access, and computer files; no expectation of privacy

The Company owns the rights to all data and files in any computer, network, or other information system used in the Company and to all data and files sent or received using any company system or using the Company's access to any computer network, to the extent that such rights are not superseded by applicable laws relating to intellectual property. The Company also reserves the right to monitor electronic mail messages (including personal/private/instant messaging systems) and their content, as well as any and all use by employees of the Internet and of computer equipment used to create, view, or access e-mail and Internet content. Employees must be aware that the electronic mail messages sent and received using Company equipment or Company-provided Internet access, including web-based messaging systems used with such systems or access, are not private and are subject to viewing, downloading, inspection, release, and archiving by Company officials at all times. The Company has the right to inspect any and all files stored in private areas

of the network or on individual computers or storage media in order to assure compliance with Company policies and state and federal laws. No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the employee or an appropriate Company official.

The Company uses software in its electronic information systems that allows monitoring by authorized personnel and that creates and stores copies of any messages, files, or other information that is entered into, received by, sent, or viewed on such systems. There is no expectation of privacy in any information or activity conducted, sent, performed, or viewed on or with Company equipment or Internet access. Accordingly, employees should assume that whatever they do, type, enter, send, receive, and view on Company electronic information systems is electronically stored and subject to inspection, monitoring, evaluation, and Company use at any time. Further, employees who use Company systems and Internet access to send or receive files or other data that would otherwise be subject to any kind of confidentiality or disclosure privilege thereby waive whatever right they may have to assert such confidentiality or privilege from disclosure. Employees who wish to maintain their right to confidentiality or a disclosure privilege must send or receive such information using some means other than Company systems or the company-provided Internet access.

The Company has licensed the use of certain commercial software application programs for business purposes. Third parties retain the ownership and distribution rights to such software. No employee may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software. Violation of this policy can lead to disciplinary action, up to and including dismissal.

Confidentiality of electronic mail

As noted above, electronic mail is subject at all times to monitoring, and the release of specific information is subject to applicable state and federal laws and Company rules, policies, and procedures on confidentiality. Existing rules, policies, and procedures governing the sharing of confidential information also apply to the sharing of information via commercial software. Since there is the possibility that any message could be shared with or without your permission or knowledge, the best rule to follow in the use of electronic mail for non-work-related information is to decide if you would post the information on the office bulletin board with your signature.

It is a violation of Company policy for any employee, including system administrators and supervisors, to access electronic mail and computer systems files to satisfy curiosity about the affairs of others, unless such access is directly related to that employee's job duties. Employees found to have engaged in such activities will be subject to disciplinary action.

Electronic mail tampering
Electronic mail messages received should not be altered without the sender's permission; nor should electronic mail be altered and forwarded to another user and/or unauthorized attachments be placed on another's electronic mail message.

Policy Statement for internet/intranet browser(s)
The Internet is to be used to further the Company's mission, to provide effective service of the highest quality to the Company's customers and staff, and to support other direct job-related purposes. Supervisors should work with employees to determine the appropriateness of using the Internet for professional activities and career development. The various modes of Internet/Intranet access are Company resources and are provided as business tools to employees who may use them for research, professional development, and work-related communications. Limited personal use of Internet resources is a special exception to the general prohibition against the personal use of computer equipment and software.

Employees are individually liable for any and all damages incurred as a result of violating company security policy, copyright, and licensing agreements.

All Company policies and procedures apply to employees' conduct on the Internet, especially, but not exclusively, relating to: intellectual property, confidentiality, company information dissemination, standards of conduct, misuse of company resources, anti-harassment, and information and data security.

Personal electronic equipment
The Company prohibits the use or possession in the workplace of any type of camera phone, cell phone camera, digital camera, video camera, or other form of image- or voice-recording device without the express permission of the Company and of each person whose image and/or voice is/are recorded. Employees with such devices should leave them at home unless expressly permitted by the Company to do otherwise. This provision does not apply to designated Company personnel who must use such devices in connection with their positions of employment.

Employees should not bring personal computers or data storage devices (such as floppy disks, CDs/DVDs, external hard drives, flash drives, "smart" phones, iPods/iPads/iTouch or similar devices, mobile computing devices, or other data storage media) to the workplace or connect them to Company electronic systems unless expressly permitted to do so by the Company. Any employee bringing a personal computing device, data storage device, or image-recording device on company premises thereby gives permission to the Company to inspect the personal computer, data storage device, or image-recording device at any time with personnel of the company's choosing and to analyze any files, other data, or data storage devices or media that may be within or connectable to the personal computer or image-recording device in question. Employees who do not wish such inspections to

be done on their personal computers, data storage devices, or imaging devices should not bring such items to work at all.

Violation of this policy, or failure to permit an inspection of any device covered by this policy, shall result in disciplinary action, up to and possibly including immediate termination of employment, depending upon the severity and repeat nature of the offense. In addition, the employee may face both civil and criminal liability from the Company, from law enforcement officials, or from individuals whose rights are harmed by the violation.

10. Change control policy

This policy applies to all parties operating within the company's network environment or utilizing Information Resources. It covers the data networks, LAN servers and personal computers (stand-alone or network-enabled), located at company offices and company production related locations, where these systems are under the jurisdiction and/or ownership of the company or subsidiaries, and any personal computers, laptops, mobile device and or servers authorized to access the company's data networks. No employee is exempt from this policy.

Purpose

The purpose of this policy is to establish management direction and high-level objectives for change management and control. This policy will ensure the implementation of change management and control strategies to mitigate associated risks such as:

- Information being corrupted and/or destroyed;
- Computer performance being disrupted and/or degraded;
- Productivity losses being incurred; and
- Exposure to reputational risk.
- Operational Procedures.

Operational procedures

The change control process shall be formally defined and documented. A change control process shall be in place to control changes to all critical company information resources (such as hardware, software, system documentation and operating procedures). This documented process shall include management responsibilities and procedures. Wherever practicable, operational and application change control procedures should be integrated.

- At a minimum the change control process should include:
- Logged Change Requests.
- Identification, prioritization and initiation of change.
- Proper authorisation of change.
- Requirements analysis.
- Inter-dependency and compliance analysis.

- Impact Assessment.
- Change approach.
- Change testing.
- User acceptance testing and approval.
- Implementation and release planning.
- Documentation.
- Change monitoring.
- Defined responsibilities and authorities of all users and IT personnel.
- Emergency change classification parameters.

Documented change
All change requests shall be logged whether approved or rejected on a standardised and central system. The approval of all change requests and the results thereof shall be documented. A documented audit trail, maintained at a Business Unit Level, containing relevant information shall be maintained at all times. This should include change request documentation, change authorisation and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorised personnel.

Risk management
A risk assessment shall be performed for all changes and dependent on the outcome, an impact assessment should be performed.

The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.

Change classification
All change requests shall be prioritised in terms of benefits, urgency, effort required and potential impact on operations.

Testing
Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.

Changes affecting SLA‘s
The impact of change on existing SLA’s shall be considered. Where applicable, changes to the SLA shall be controlled through a formal change process which includes contractual amendments.

Version control

Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies.

Approval
All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorised user, the impact assessment was performed and proposed changes were tested.

Communicating changes
All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change. Users shall be required to make submissions and comment prior to the acceptance of the change.

Implementation
Implementation will only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes.

Fall back
Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert back to what they were prior to implementation of changes.

Documentation
Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies.

Information resources documentation is used for reference purposes in various scenarios i.e. further development of existing information resources as well as ensuring adequate knowledge transfer in the event of the original developer and/or development house being unavailable. It is therefore imperative that information resources documentation is complete, accurate and kept up to date with the latest changes. Policies and procedures, affected by software changes, shall be updated on completion of each change.

Business continuity plans (BCP)
Business continuity plans shall be updated with relevant changes, managed through the change control process. Business continuity plans rely on the completeness,

accuracy and availability of BCP documentation. BCP documentation is the road map used to minimise disruption to critical business processes where possible, and to facilitate their rapid recovery in the event of disasters.

Emergency changes
Specific procedures to ensure the proper control, authorisation, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.

Change monitoring
All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

A summary of the roles and responsibilities of various stakeholders during a change management process is enlisted below:

Members of the Board

- Members of the Board shall ensure that the necessary information security controls are implemented and complied with as per this policy.

Information Security Manager

- Establish and revise the information security strategy, policy and standards for change management and control with input from interest groups and subsidiaries;
- Facilitate and coordinate the necessary counter measures to change management and control initiatives and evaluate such policies and standards;
- Establish the security requirements for change management and control directives and approval of the change management and control standards and change control/ version control products;
- Coordinate the overall communication and awareness strategy for change management;
- Acts as the management champion for change management and control;
- Provide technical input to the service requirements and co-ordinate affected changes to SLA's where applicable.
- Establish and coordinate appropriate interest group forums to represent, feedback, implement and monitor change management and control initiatives; and
- Coordinate the implementation of new or additional security controls for change management.

Operations Manager

- Implement, maintain and update the change management and control strategy, baselines, standards, policies and procedures with input from all stakeholders;
- Approve and authorise change management and control measures on behalf of the StratAgile
- Ensure that all application owners are aware of the applicable policies, standards, procedures and guidelines for change management and control;
- Ensure that policy, standards and procedural changes are communicated to applicable owners and management forums;
- Appoint the necessary representation to the interest groups and other forums created by each company for Information Security Management relating to change management and control;
- Establish and revise the information security strategy, policy and standards for change management and control;
- Facilitate and coordinate the necessary change management and control initiatives within each company;
- Report and evaluate changes to change management and control policies and standards;
- Coordinate the overall communication and awareness strategy for change management and control;
- Coordinate the implementation of new or additional security controls for change management and control
- Review the effectiveness of change management and control strategy and implement remedial controls where deficits are identified;
- Provide regular updates on change management and control initiatives and the suitable application;
- Evaluate and recommend changes to change management/ version control solutions; and
- Coordinate awareness strategies and rollouts to effectively communicate change management and control mitigation solutions in each company.
- Establish and implement the necessary standards and procedures that conform to the Information Security policy;
- Responsible for approving, authorising, monitoring and enforcing change management initiatives and related security controls within all companies and divisions;
- Ensure that all solution owners are aware of policies, standards, procedures and guidelines for change management and control.
- Ensure the compliance of this policy and report deviations to the Information Manager.

IT Service Provider

- Shall comply with all change management and control statements of this policy.

Solution Owners

- Shall comply with all information security policies, standards and procedures for change management and control; and
- Report all deviations.

11. Data privacy policy and data protection rule compliance

StratAgile complies with Guidance on the PDPA (Privacy data protection rule) in Singapore. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organization. This policy covers (insert types of people as appropriate – employed staff, trustees, volunteers). In line with the Personal Data (Privacy) Ordinance principles, StratAgile will ensure that personal data will:

- Be obtained fairly & lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specific and lawful purpose
- Be adequate, relevant but not excessive
- Be accurate and kept up to date
- Not be held longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures

The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.

The Ordinance on data protection suggests six key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e.

- Purpose and manner of collection of personal data.
- Accuracy and duration of retention of personal data.
- Use of personal data.
- Security of personal data.
- Information to be generally available.
- Access to personal data.

To meet the responsibilities (staff, partners and other agencies) will:

- Ensure any personal data is collected in a fair and lawful way.
- Explain why it is needed at the start
- Ensure that only the minimum amount of information needed is collected and used.
- Ensure the information used is up to date and accurate.
- Review the length of time information is held.
- Ensure it is kept safely.
- Ensure the rights people have in relation to their personal data can be exercised.

We will ensure that:

- Everyone managing and handling personal information is trained to do so.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in line with our procedures.
- Queries about handling personal information will be dealt with swiftly and politely.
- Training and awareness raising about the Data Protection Act

This policy will be reviewed once in a year to ensure it remains up to date and compliant with the law.

12. IT asset control and disposal policy

All employees and personnel that have access to organizational computer systems must adhere to the IT asset control policy defined below in order to protect the security of the network, protect data integrity, and protect and control computer systems and organizational assets. The asset control policy will not only enable organizational assets to be tracked concerning their location and who is using them but it will also protect any data being stored on those assets. This asset policy also covers disposal of assets.

IT assets should not be confused with nor tracked with other organizational assets such as furniture. One of the main reasons to track IT assets other than for property control and tracking is for computer security reasons. A special IT asset tracking policy will enable the organization to take measures to protect data and networking resources.

This policy will define what must be done when a piece of property is moved from one building to another or one location to another. This policy will provide for an asset tracking database to be updated so the location of all computer equipment is known. This policy will help network administrators protect the network since they will know what user and computer is at what station in the case of a worm infecting the

network. This policy also covers the possibility that data on a computer being moved between secure facilities may be sensitive and must be encrypted during the move.

Purpose & responsibility

This policy is designed to protect the organizational resources on the network by establishing a policy and procedure for asset control. These policies will help prevent the loss of data or organizational assets and will reduce risk of losing data due to poor planning. The CIO or CIO designate is ultimately responsible for the development, implementation and enforcement of this policy.

IT asset types

This section categorized the types of assets subject to tracking.

- Desktop workstations
- Laptop mobile computers
- Mobile phones and tablets
- Printers, Copiers, FAX machines, multifunction machines
- Handheld devices including Tablets
- Scanners
- Servers
- Firewalls
- Routers
- Switches
- Memory devices

Assets tracked

Assets which cost less than HKD 250 shall not be tracked specifically including computer components such as video cards or sound cards. However, assets which store data regardless of cost shall be tracked. These assets include:

- Hard Drives
- Temporary storage drives
- Tapes with data stored on them including system backup data.
- Although not specifically tracked, other storage devices including CD ROM disks and floppy disks are covered by this policy for disposal and secure storage purposes.

Small memory devices

Small memory storage assets will not be tracked by location. These assets include:

- CD ROM disks
- Memory sticks

If these types of devices are permitted for some employees, the trustee of the device must sign for receipt of these devices in their possession. All employees must also agree to handle memory sticks, floppy disks, and CD ROM disks in a responsible manner and follow these guidelines:

- Never place sensitive data on them without authorization. If sensitive data is placed on them, special permission must be obtained and the memory device must be kept in a secure area.
- Never use these devices to bring executable programs from outside the network without authorization and without first scanning the program with an approved and updated anti-virus and malware scanner. Any program brought into the network should be on the IT department list of approved programs.

The Memory Device Trustee agreement allows employees to sign for receipt of these devices and agree to handle these devices in accordance with the terms of this policy. This form must be submitted by all employees that will work with any organizational data when the employee begins working for the organization. It will also be submitted when employee receives one or more memory sticks, temporary storage drives, or data backup drives.

Asset tracking requirements

- All assets must have an ID number. Either an internal tracking number will be assigned when the asset is acquired or the use of Manufacturer ID numbers must be specified in this policy.
- An asset tracking database shall be created to track assets. It will include all information on the Asset Transfer Checklist table and the date of the asset change.
- When an asset is acquired, an ID will be assigned for the asset and its information shall be entered in the asset tracking database.

Transfer procedure

Asset Transfer Checklist - When an asset type listed on the Asset Types list is transferred to a new location or trustee, the IT Asset Transfer Checklist must be filled out by the trustee of the item and approved by an authorized representative of the organization. The trustee is the person whose care the item is in. If the item is a workstation, then the trustee is the most common user of the workstation. For other equipment, the trustee is the primary person responsible for maintenance or supervision of the equipment. The trustee must fill out the Asset Transfer Checklist form and indicate whether the asset is a new asset, moving to a new location, being transferred to a new trustee, or being disposed of. The following information must be filled in:

- Asset Type
- ID number
- Asset Name
- Current Location
- Designated Trustee
- New Location
- New Trustee
- Locations of Sensitive Data

Once the trustee fills out and signs the Asset Transfer Checklist form an authorized representative must sign it.

Data entry - After the Asset Transfer Checklist is completed, it will be given to the asset tracking database manager. The asset tracking database manager will ensure that the information from the forms is entered into the asset tracking database within one week.

Checking the database - Managers who manage projects that affected equipment location should check periodically to see if the assets that recently were moved were added to the database. The database should provide a recent move list which can be easily checked. Managers should check the database weekly to be sure assets moved within the last 2 or 3 weeks are included in the database.

Asset transfers

This policy applies to any asset transfers including the following:

- Asset purchase
- Asset relocation
- Change of asset trustee including when an employee leaves or is replaced.
- Asset disposal, including:
    - Asset returned to manufacturer or reseller due to
    - warranty return.
    - Leased asset returned to Lessor.

In all these cases the asset transfer checklist must be completed.

Media sanitization

When transferring assets to another party, any confidential information on the device must be protected and/or destroyed. The method of data destruction is dependent on the sensitivity of the data on the device and the next user of the device (within the organization and its controls or outside the organization).

Asset disposal

Asset disposal is a special case since the asset must have any sensitive data removed during or prior to disposal. The manager of the user of the asset must determine what the level of maximum sensitivity of data stored on the device is. Below is listed the action for the device based on data sensitivity according to the data assessment process.

- None (Unclassified) - No requirement to erase data but in the interest of prudence normally erase the data using any means such as sanitization, physical destruction or degaussing.
- Low (Sensitive) - Erase the data using any means such as electronic sanitization, physical destruction or degaussing.

- Medium (Confidential) - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques.
- High (Secret) - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques. Approved technologies are to specified in a Media Data Removal Procedure document by asset type including:
    - Memory stick
    - CD ROM disk
    - Storage tape
    - Hard drive.
    - RAM memory
    - ROM memory or ROM memory devices.

Media use

This policy defines the types of data that may be stored on removable media and whether that media may be removed from a physically secure facility and under what conditions it would be permitted. Removable media includes:

- Memory stick
- CD ROM disk
- Storage tape

Below is listed the policy for the device based on the rated data sensitivity of data stored on the device according to the data assessment process.

- Unclassified - Data may be removed with approval of the first level manager and the permission is perpetual for the employee duration of employment unless revoked. The device may be sent to other offices using any public or private mail carrier.
- Sensitive - Data may only be removed from secure areas with the permission of a director level or higher level of management and approvals are good for one time only.
- Confidential - The data may only be removed from secure areas with permission of a Vice -president or higher level of management. There must be some security precautions documented for both the transport method and at the destination.
- Secret - - The data may only be removed from secure areas with the permission of the President or higher level of management. There must be some security precautions documented for both the transport method and at the destination.
- Top secret - The data may never be removed from secure areas.

Enforcement

Since data security and integrity along with resource protection is critical to the operation of the organization, employees that do not adhere to this policy may be

subject to disciplinary action up to and including dismissal. Any employee aware of any violation of this policy is required to report it to their supervisor or other authorized representative.

Employee training and acknowledgment of policy
Each employee in the organization is expected to be aware of current policies and procedures related to IT Security and shall be trained on these policies and procedures on at least an annual basis. Employees are required to sign an acknowledgment that they are aware of the policy and will meet its requirements.

13. Patch management policy

Scope
This policy applies to workstations or servers owned or managed by StratAgile. This includes systems that contain company or customer data owned or managed by StratAgile regardless of location. The following systems have been categorized according to management:

- Unix/Solaris servers managed by Unix Engineering Team.
- Microsoft Windows servers managed by Windows Engineering Team.
- Workstations (desktops and laptops) managed by Workstation Imaging Team.

Policy
Workstations and servers owned by StratAgile must have up-to-date operating system security patches installed to protect the asset from known vulnerabilities. This includes all laptops, desktops, and servers owned and managed by StratAgile.

Workstations
Desktops and laptops must have automatic updates enabled for operating system patches. This is the default configuration for all workstations built by StratAgile Any exception to the policy must be documented and forwarded to the CIO's office.

Servers
Servers must comply with the minimum baseline requirements that have been approved as a part of the project. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the StratAgile asset and the data that resides on the system. Any exception to the policy must be documented and forwarded to the GSO for review.

Roles and responsibilities

- Unix Engineering will manage the patching needs for the Linux, UNIX, and Solaris servers on the network.
- Windows Engineering will manage the patching needs for the Microsoft Windows servers on the network.

- Workstation Imaging will manage the patching needs of all workstations on the network.
- Information Security is responsible for routinely assessing compliance with the patching policy and will provide guidance to all groups in issues of security and patch management.
- The CIO/CIO designate is responsible for approving the monthly and emergency patch management deployment requests.

Monitoring and reporting
Active patching teams noted in the Roles and Responsibility are required to compile and maintain reporting metrics that summarize the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk. These reports shall be made available to Information Security and Internal Audit upon request.

Enforcement
Implementation and enforcement of this policy is ultimately the responsibility of all employees at StratAgile Information Security and Internal Audit may conduct random assessments to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the StratAgile issue tracking system and support teams shall be dispatched to remediate the issue. Repeated failures to follow policy may lead to disciplinary action.

14. Anti-malware policy

StratAgile is obliged to make sure its IT systems and other facilities are secure and not subject to improper use. This policy sets out the responsibilities of all users, including users of privately owned devices that connect to the StratAgile facilities, in relation to malicious software. These measures do not guarantee security, but they will help to significantly reduce the risk of widespread virus infection in the organisation. All users need to read, understand, and comply with this Policy.

The word ‘malware’ is used collectively to denote many types of malicious software, including viruses, worms, Trojans, macros, mail bombs and rootkits.
A virus is a piece of self-replicating computer program code that is designed to destroy or damage digital information, or to steal user or business data.
There are many potential sources of malicious software, including websites, social media, USB memory sticks, unsolicited CDs, electronic mail, and software or documents copied over networks such as the campus network or the internet.

Objectives
- The objectives of this document are:
- To set out user responsibilities with regard to malicious software prevention.

- To set out the rules governing the application and use of malicious software prevention systems at the StratAgile.

Applicability

This Policy applies to all users, including privately owned devices that connect to the StratAgile. IT facilities. By following this Policy, users will help to protect themselves and other StratAgile users against malicious software. The StratAgile IT Regulations, on which this Policy expands, require everyone to take the practical steps needed to keep this protection active and up to date.

Policy statements

- All StratAgile personal computers and servers that are connected to the StratAgile network or otherwise using the IT facilities must run an approved and up-to-date anti-virus product that continually monitors for malicious software (viruses, worms, etc.).
- All personal computers, devices and servers connected to the StratAgile network must run a version of the Operating System and installed applications with the latest available patches applied.
- Computers and tablets supported by StratAgile will be supplied with an anti-virus product if appropriate and with automatic updating for it and for the Operating System and applications.
- Any non- StratAgile owned devices (BYOD) must run an appropriate anti-virus product. Users who do not choose a recommended anti-virus product must make their own adequate anti-virus protection arrangements for their privately owned devices.
- Do not try to uninstall or disable anti-virus software. Any messages suggesting that anti-virus protection has been disabled should be investigated immediately.
- If users experience difficulties with a recommended anti-virus product, requests for technical support may be made quickly.
- The StratAgile IT Regulations prohibit any activity intended to create and / or distribute malicious code (viruses, worms, etc.) on the network or IT facilities. However, when requested to do so by Exeter IT staff in order to aid investigations, users may send suspected malware using a method that does not allow the malware to propagate / spread.
- The StratAgile reserves the right to disconnect any device from the network if an infection is found or suspected. The device will be disconnected until the infection is removed and suitable preventative tools have been installed on the device.
- Email attachments may be scanned by an antivirus product before delivery.
- Check the authenticity of attachments / software to be installed from internet sources. Do not install applications that arrive on unsolicited media.

- Individuals may be subject to disciplinary action if this Policy is breached.

15. Cloud computing security policy

Proper security in a cloud environment requires specialized practices and processes at both the physical and virtualization levels. Following are some key features to look for when evaluating a cloud services provider:

Physical security at data centers

- 24x7x365 manned main entrance
- Secured access doors and elevator banks
- Monitored security cameras
- Motion and camera sensors
- Visitor logs for cages
- Key-locked cages and cabinets

Infrastructure security

In public cloud environments, multi-tenancy can pose a security risk if proper isolation measures are not put into place to securely separate data and resources. If you're looking for more security through a private cloud, be sure to look for the following requirements

- ***Availability***: Redundancy should be built into every layer of the technology infrastructure to minimize the risk of unplanned downtime.
- ***Secure separation***: Ensure that your cloud provider will use secure separation to isolate your silo and resources from other cloud customers.
- ***Service assurance*****:** Computing, networking and storage resources should be readily available to you as needed to deliver top performance and accommodate fluctuations in user demands.
- ***Management and monitoring***: Work closely with your cloud services provider to ensure they will have comprehensive control and extensive visibility over your cloud infrastructure at all times. You need to ensure it is highly secure, your environment is separated and you receive the highest level of service.

Policies and procedures

Audit the service provider around the policies and procedures they have in place for access control to your cloud environment. Following are some must-haves:

- Access Control Policy: How is access to and control of the storage, virtualization and network infrastructures managed? What protocols are in place for monitoring, granting access and logging changes to client information systems?

- Information Security Management Policy: What safeguards does the provider have in place to protect against physical and virtual threats? How are security violations and incidents reported and managed? What information does the provider collect about clients and how is it handled? Has the provider ever had a security breach, and if so, what was the outcome?
- Employee, Visitor and Contractor Physical Security Policy: What practices are in place for monitoring employees, visitors and contractors while on premise (office or data center)? What background verification, screening agreements and employment agreements are established?

Denture Security Practices

There are six fundamental security practices to be followed whether using on-premise infrastructure or a cloud service.

- Passwords are essential, but simply having one isn't enough. Remind users not to leave passwords on sticky notes or under their keyboards. One way to remember a new password is to use it immediately and often. Also, don't change a password before leaving for vacation or on a Friday, as you're more likely to forget it.
- Create strong passwords. A good password is easy for a user to remember but hard for someone to guess. Think about substituting letters for numbers and vice versa. Also, be sure to change your password often - best practice is every 30-90 days.
- Remember to lock the doors. Propping open a door to expedite FedEx deliveries or get fresh air is fine, but keep an eye on who uses the door and be sure to make sure it is locked before leaving for the day and when the front desk is not staffed.
- Laptops are easy prey. About 97 percent of stolen computers are never recovered, according to the FBI. The latest designer bag is the first tip-off to a would-be thief. Also, do not leave your laptop unattended while in an airport, hotel or conference.
- Add local security measures. Further security measures can be taken locally on laptops through the use of portable physical locking mechanisms, active directory, biometrics, and encryption. Local encryption software can provide automated, real-time data encryption that can help protect information even if a laptop is lost or stolen.
- Mobility devices need protection too. Just as laptops require passwords, so do PDAs.
- Scams and hoaxes
- Many spam emails are sent with dire warnings about messages with topical subjects or attachments. The receiver is often asked to forward the email to all colleagues and friends around the globe. If you are unsure whether an email you receive is a hoax or scam, you can check it at www.snopes.com. Do not forward these messages on. If you receive such a message, just delete it.

- Some websites you visit will suggest your PC or tablet is infected with a new virus and hence you need to run / install / purchase their anti-virus software. Do not click this message. Instead, check that you have the latest signatures and updates in your existing anti-virus software and then run a manual scan.
- If you download a fake anti-virus application, or think that your device has a virus, please report this to the Contact us or to local IT staff as soon as possible, because it will be much easier to remove if reported promptly.

16. Backup policy and procedures

Purpose

The unprecedented growth in data volumes has necessitated an efficient approach to data backup and recovery. This document is intended to provide details on the stipulations of data backup and retrieval operations to the client.

Scope

The intended recipients of this policy are business divisions and client project owners that house the data within StratAgile Data Center.

Policy

Information Technology recognizes that the backup and maintenance of data for servers are critical to the viability and operations of the respective departments. It is essential that certain basic standard practices be followed to ensure that data files are backed up on a regular basis.

Procedure

The backup server currently deployed has an LTO 3 backup tape device and a Virtual Tape Library (DL 710) attached to it. The DL 710 provides us with disk-based backup and also allows us to do a disk-to-disk-to-tape backup. The type of backup varies with the model of the server and the volume of data to be backed up. A cloud based backup is also provisioned if the project necessitates the same.

The backup software used to control the backup processes. The Systems Support team ensures that all backups are completed successfully and reviews the backup process on all servers daily. Logs are maintained to verify the amount of data backed up and the unsuccessful backup occurrences.

Backup content

The content of data backed up varies from server-to-server. The primary data that will be backed up are: Data files designated by the respective owners of the servers and in some instances System Data (Applications files for the server and other selected software installed on the server). Data to be backed up will be listed by location and specified data sources. This will be stipulated in a separate document called “Data

Sources Manifest". Because it is impractical for the Systems Support to back up every bit of data stored on the servers, the only data that Systems accepts responsibility for is the data which is explicitly listed in the "Data Source Manifest".

Backup types

Backup of servers will occur every day after regular business hours.

- Full backup: Includes all the source files. This method ignores the file's archive bit until after the file is backed up. At the end of the job, all files that have been backed up have their archive bits turned off. Only one full backup will be done once a week followed by differential and/or incremental.
- Differential backups: Includes files that have been changed since the last Full (Clear Archive Bit) or Incremental backup. If the archive bit is on, the file is backed up, and archive bit is not turned off. The next time an incremental backup is done, this file is skipped (unless it is modified again).
- Incremental backups: Includes only files that have changed since the last Full (Clear Archive Bit) or Incremental backup. The next time an incremental backup is done, this file is skipped (unless it is modified again).
- We use the GFS (Grandfather-Father-Son) rotation for backups.
- Daily backups (Son) take place on a five day rotation.
- Weekly backups (Father) take place on a five week rotation.
- Monthly backups of high availability servers occur the last calendar day of the month and are on a twelve month rotation.
- Special backups may be made for longer retention periods during special situations such as system upgrades and major projects.

Offsite storage of tapes

Any data that requires offsite storage must be requested by the owner of the server. The tapes containing said data will be stored offsite for a period of one month by Commercial Record Center.

Data Source Manifest			
Date :		Server Name:	

Type of Backup Agent Needed

☐	Windows	Version:		Type:	
☐	Linux	Version:		Type:	
☐	Unix	Version:		Type:	

List of Files/Folders to be Backed Up

Backup Client and Policy

Backup Client Installed On Client Server:	☐ Yes							☐ No								
Backup Policy for Client Server:	☐ F ☐ D ☐ I	MON	☐ F ☐ D ☐ I	TUE	☐ F ☐ D ☐ I	WED	☐ F ☐ D ☐ I	THU	☐ F ☐ D ☐ I	FRI	☐ F ☐ D ☐ I	SAT	☐ F ☐ D ☐ I	SUN		
Run Schedule for Policy:	AM:							PM :								

Only One Full (F) followed by either a Differential (D) or an Incremental (I)

Retention and Offsite

Retention Period for Backup:	☐ 1 Week	☐ 2 Weeks	☐ 1 Month	☐ 2 Months
Offsite Storage:	☐ Yes		☐ No	

Signatures

Requestor's Signature:		Date :	
System/Backup Administrator Signature:		Date :	

17. Production and testing environments policy

Any change to a system, including required configuration changes, upgrades, or system updates can break a working system. At the same time every deployment and system requires configuration changes, upgrades and updates. Balancing these requirements presents a core problem in systems administration n and necessitates the Production and Testing environment.

Ensuring a stable production environment requires appropriate testing infrastructure and sufficient policies and automation around application deployment to ensure that deploying new software or running software updates are reliable and do not require manual intervention.

This document addresses both halves of this problem–the infrastructure and the policy–and includes different method, techniques, and strategies that make it possible for administers to ensure reliable application and system updates.

The following concepts introduce crucial components and requirements of deployment testing infrastructure.

Change control
Systems that monitor production environments for changes and modifications and alert administrators of intrusions. As a result, change control is typically used as a security measure. At the same time, sometimes change control can refer to policies that control how changes propagate to the production systems, and change control tools can be used to enforce testing and staging policies.

Development environment
A deployment of the application or application for exploratory and development use. While these environments resemble the production environment, they are often much smaller in terms of available resources and data. Development systems are what administrators and developers use to test and experiment with changes before implementing them in the test environment. These may run in virtual machines that resemble the test environment, or on developer's laptops.

Fire call
A method used by administrators to get emergency administrative access in deployments where no individual has "root" or administrative access. This both allows emergency work on a deployment and works to allow administrators to avoid accidentally modifying systems.

Production environment
The servers that clients actually interact with. These servers are doing the actual work of the deployment. Administrators should modify instances and applications running in this environment as minimally as possible.

Rollback
Refers to the process of "unwinding" a change applied to a production environment that reverts the environment to a previous known working state.

Test environment
Servers that provide a very accurate reproduction of the production environment. Use this as a final testing substrate before implementing changes or updates on the production system. Sometimes it's not feasible to fully replicate production environments in test, but the differences ought to be minimal so that differences between the test and production environments don't cause unexpected problems. Virtualized production and test environments make it easier to more accurately

replicate the production environment in test. Some organizations and resources refer to test environments as “staging environments.”

Testing infrastructure

- Having a secure and reliable testing environment is essential, and without one it’s impossible to verify that changes are “good” before deploying them. However, the extent of your testing, and the tolerances based on the administrative requirements and from stakeholder needs.
- When configuring your test environments consider the following basic requirements:
- Testing needs to be easy. In order to ensure that you and your developers will rigorously test changes and updates, testing changes needs to be trivially easy. In addition to any other interface, it must be easy to restart and reset the environment to “base configurations,” to “back out” of bad configurations easily.
- Usability in this case also mandates some measure of performance. If it takes too long to reset an environment, or if the environment is too slow for any number of reasons, test environments are less likely to get used.
- Using a deployment automation system, either something custom based on build scripts, make files, or something similar to ensure consistency.
- Use virtualization to isolate environments. Tools like “Vagrant great for this purpose
- While the term “stakeholders,” comes to us from the world of management and bears a certain amount of distaste in the minds of most systems administrators, it’s useful to be able to recognize where operational needs originate.
- For some services, the administrators are the main consumers or stakeholders. Directory services, management tools and databases, logging and monitoring systems, and so forth are all primarily used to support infrastructure. For other systems: file servers, web-based applications, and so forth, other groups dictate operational requirements and tolerances.

Deployment processes and policy

- Once you have the infrastructure to perform testing, it’s important to ensure that you do perform tests. Software developers use continuous integration systems to automate tests, and in some cases you can automate testing for deployments work using a similar method. Often, the kind of testing that administrators need to do is more complex.
- Where programmers can often write test cases that verify the behavior of a program, operational testing requires not only that a single program behave correctly, but rather that an entire collection of programs behave correctly together in a specific environment. In the process of testing it’s important to be able to affirmatively answer the following questions:
- Will this upgrade or change break any dependent service? For example, does upgrading an LDAP (directory) service impact email services?

- Does this upgrade or change introduce any (new) client compatibility issues? For instance, would switching to SSL SNI for HTTPS break compatibility with clients that you must support?
- Does one change (i.e. deploying a new version of an existing application,) require configuration changes (i.e. the installation of a library, changes to networking rules, or changes to files beyond what's contained in the upgrade itself?
- There are a number of different policies at the organizational level that can help you support testing requirements. Typically these standards and practices revolve around making testing easier, less burdensome, more automated, and more integrated into existing workflows. For instance, consider the following:
- Mandate reviews and sign offs for changes. Make sure that except for fire call situations, more than one administrator is responsible for reviewing and signing off on any change. This is not possible in small teams and for some sets of changes. Also, while these multi-sign off policies lengthen timescales considerably fresh eyes and different perspectives are quite useful and prevent many bugs and issues.
- If you manage configuration and deployment programmatically, all changes to the production system must be code reviewed before propagating it to the production system.
- Integrate testing into other tools and workflows. Including testing infrastructure that is either automated (of the "continuous integration" type,) connected to change requests and ticketing, or integrated with version control tools.
- Provide local preliminary ("dev") testing. If you and your developers and administrators have an easy way to test changes, and become familiar with software, it's more likely that you and other administrators will test code regularly and that you'll do experimentation with test and production environments. Lower barriers to entry are key to ensuring that developers use these systems.

Rollback

- Controlling access to resources and providing testing environments is crucial for maintaining production systems. While there are no substitutes for implementing policies and procedures to protect deployments and ensure that updates and upgrades go smoothly, it's important to provide a rollback option when an upgrade has unforeseen consequences. These allow you to return a deployment to a previous "known working state," if something breaks.
- There are a few methods/technologies that you can use to provide rollbacks:
- Use LVM or some other file-system or block level snapshotting tool to create a backup of a system before applying the change. If something goes wrong with the upgrade process, you can roll back to a previous state.
- If ruining in a virtualized environment, duplicate the instance, and upgrade the server, and perform a manual failover (swap the IP addresses) if you need a

rollback. Ensure that modifying the IP address works (i.e. send appropriate ARP requests.)

- Use a script to apply the changes, and write a rollback function to reverse all changes that you apply, and test both in your test environment.
- In general, you should script and automate rollbacks–like deployment processes–so that it's possible to back out of an update without needing to remember the sequence of operations that you performed to update the system. Sometimes this is reasonably complicated, as in the case of operating system updates and upgrades. In other situations it may be as simple as changing a symbolic link, as in some application deployment schemes. Above all, remember to be as rigorous about rollbacks and testing as you are about the updates themselves.

Change Control

- Change control software monitors systems and applications to insure that configuration remains constant and that configuration changes are not implemented outside of normal change policies. This is typically implemented as a special kind of monitoring or intrusion detection system.
- While it's important to develop policies regarding changes to production systems, it's also important to provide some method to ensure that the system or systems remain intact and that some untracked change to the production system don't either impact the integrity of the system or affect the operational conditions of the systems. Change control may help you address this requirement.
- Change control is a difficult problem, and it's beyond the scope of this article. As a security practice, it's reactive and reliable change control is difficult to implement effectively. For many (or most) deployments, the kinds of typical intrusion detection solutions used for change control are overblown.
- Even if your deployment does not merit a change control solution, collecting some "change control data" may be useful. For instance, log INS and daemon restarts may indicate some tampering, and your logging and monitoring system should track these events. Also, use privilege escalation systems like suds that provide more logging rather than shared privileged accounts for administrative tasks.
- Typically if a user has the access to be able to impact a production system, they also have the ability to affect the change control monitor itself. Beyond this, change control systems cannot prevent intrusions or unwanted modifications except through Foucauldian methods, and can only report on them after the fact.

Policy, auditing, and production testing

- Maintaining separation between test and production environments, as well as a usable and reliable deployment systems is not a significant technological problem: it's a social and policy problem. To properly address these concerns you need some required infrastructure, but really need to develop sufficient

policies and procedures that make sense in the context of your environment and that all of your administrators and operators can work within.

- Devising policies that are functional from an administrative use perspective is a requisite first step, but it's also important to ensure that the policy is also sufficiently flexible. A rigid policy may not allow for timely administrative response to unforeseen bugs or system events, which can be devastating. So called "fire call" systems are useful for providing an emergency exception: again, this is a thin technological wrapper around a policy problem.
- Full-scale auditing is often unworkable: of logs in large clusters, of file system changes on any system, so while some level of auditing may be useful for "covering" and protecting your systems, the truth is that it's not possible to fully audit production and test systems. In light of this, the most important aspects of maintaining sane deployment policies and practices are (in descending order :)
- Make testing infrastructure and systems available and easy to use.
- It's difficult to test effectively if there aren't properly configured test machines. Furthermore developers and administrators are unlikely to test effectively if the testing system is difficult to use.
- Make sure that testing environments resemble production systems to the greatest extent possible.
- The greater the differences between the test environment and the production environment, the less effective the test environment becomes at predicting what will happen in production.

Automate testing

- For important components use automated testing methods, either with continuous integration systems or by some other means, to ensure that most routine testing is ongoing and does not require active developer initiative.
- Create and test rollbacks, to ensure that even if an update does not go as planned, it's possible to return to a known working state.
- Limit changes to production systems.
- Use access control systems and monitoring tools to ensure that production and testing systems remain consistent and don't drift from each other.

18. IT security incident management policy

These guidelines are created to:

- Outline specific IT security incident roles and responsibilities for to be managed within the organization.
- Minimize negative consequences of information security incidents and improve the ability to promptly restore operations.
- Enable prompt incident response decisions to be made by appropriate stakeholders.

- Proactively reduce the exposure of the company or our clients to information security incidents by employing consistent incident management processes that incorporate lessons learned from past incidents.
- Satisfy federal, state, and industry regulations that require improved protection of sensitive and private information, and timely disclosure of potential breaches to affected individuals.

An information security incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of responsible use policy.

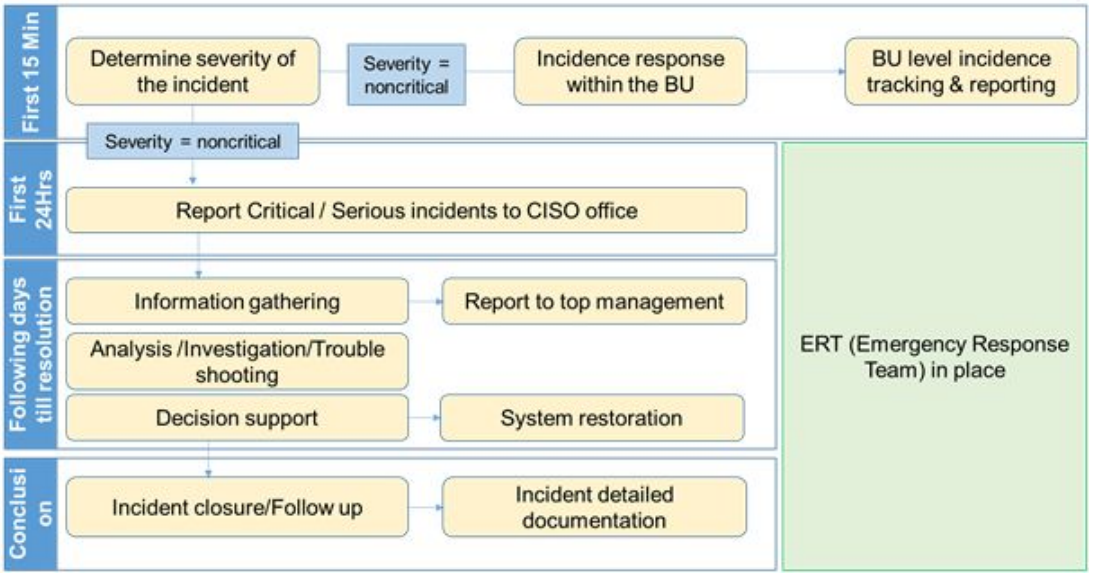
Examples of information security incidents:

- Computer system intrusion
- Unauthorized or inappropriate disclosure of sensitive institutional data
- Suspected or actual breaches, compromises, or other unauthorized access to systems, data, applications, or accounts
- Unauthorized changes to computers or software
- Loss or theft of computer equipment or other data storage devices and media (e.g., laptop, USB drive, personally owned device used for work) used to store private or potentially sensitive information
- Denial of service attack or an attack that prevents or impairs the authorized use of networks, systems, or applications
- Interference with the intended use or inappropriate or improper usage of information technology resources.

A serious incident is an incident that may pose a substantial threat to university resources, stakeholders, and/or services. An incident is designated as serious if it meets one or more of the following criteria:

- Involves potential, accidental, or other unauthorized access or disclosure of sensitive institutional information (as defined below)
- Involves legal issues including criminal activity, or may result in litigation or regulatory investigation
- May cause severe disruption to mission critical services
- Involves active threats
- Is widespread
- Is likely to be of public interest
- Is likely to cause reputational harm to the company or the clients that we work with

The incident management Lifecycle is categorised in to (i) Incident Detection and Reporting, (ii) Incident Severity Classification, (iii) Incident Response Process and Resolution and (iv) Incident detailed report. The incident lifecycle processes are depicted in Figure 1 below. They include the following:



Incident detection and reporting

The incident detection process involves observation of malicious or anomalous activity, and gathering of information that provides insight into security threats or risks. Reports of threats from sources external to company or our clients' infrastructure managed by us may also trigger an incident report. Risks, threats, and vulnerabilities. Information security incidents that are detected by any users in the system and need should be reported to the CISO's team as soon as possible but no later than 24 hours from the time they are initially detected.

Incident severity classification

Incidents that meet the Serious Incident criteria as defined in previous section must be reported to CISO's office within 1 hour. All other Non-Serious incidents are to be handled by the IT team using unit level procedures for incident response, which include incident tracking and monitoring using any automated or manual tool selected by the unit.

Incident response process

The Incident Response Process is designed to provide a high level guide for effective planning, communication, and response in the event of an IT Security Incident. Following would be the response plan when it comes to a suspected security breach incident.

- Preparation (Preparing incident response tools and IT staff for when an incident occurs)
- Identification (Determining where the incident occurred and the incident severity)
- Containment (Limiting the incident damage as quickly as possible)
- Eradication (Removing the cause of the incident)
- Recovery (Restoring affected systems to normal operational status)
- Lessons Learned (Serious Incidents)

Incident detailed reporting (serious incidents)

- All serious incidents, including incidents must be reported and documented with the following details upon completion of the resolution
- Time(s) of occurrence
- Systems/applications/devices potentially involved
- Actions taken
- Types of sensitive data that may be involved
- Potential business impacts of action or inaction
- Include contact details for business owners and technical staff involved

19. Business continuity (BCP) and disaster recovery policy (DR)

The objective of a disaster recovery plan is to ensure that you can respond to a disaster or other emergency that affects information systems and minimize the effect on the operation of the business. When you have prepared the information described in this topic collection, store your document in a safe, accessible location off site.

Goals of a disaster recovery plan.

- To minimize interruptions to the normal operations.
- To limit the extent of disruption and damage.
- To minimize the economic impact of the interruption.
- To establish alternative means of operation in advance.
- To train personnel with emergency procedures.
- To provide for smooth and rapid restoration of service.

Personnel

The following staff will be assigned for the DRP operations:

- ***Rakesh Vijayan***
  IT infrastructure & Networking Head
  (E) rakesh.v@strat-agile.com (P) +91-99955 55319
- ***Ashly Markose***
  Chief Technical Officer
  (E) ashly.m@stratagile.com (P) +65-9832 1002

Information services backup procedures

Define procedures for information services backup and share with the team

Disaster recovery procedures

For any disaster recovery plan, these three elements should be addressed.

- Emergency response procedures: To document the appropriate emergency response to a fire, natural disaster, or any other activity in order to protect lives and limit damage.
- Backup operations procedures: To ensure that essential data processing operational tasks can be conducted after the disruption.
- Recovery actions procedures: To facilitate the rapid restoration of a data processing system following a disaster.

Disaster action checklist

This checklist provides possible initial actions that you might take following a disaster.

Plan initiation:

- Notify senior management
- Contact and set up disaster recovery team
- Determine degree of disaster
- Implement proper application recovery plan dependent on extent of disaster
- Monitor progress
- Contact backup site and establish schedules
- Contact all other necessary personnel–both user and data processing
- Contact vendors–both hardware and software
- Notify users of the disruption of service

Follow-up checklist:

- List teams and tasks of each
- Obtain emergency cash and set up transportation to and from backup site, if necessary
- Set up living quarters, if necessary
- Set up eating establishments, as required
- List all personnel and their telephone numbers
- Establish user participation plan
- Set up the delivery and the receipt of mail
- Establish emergency office supplies
- Rent or purchase equipment, as needed
- Determine applications to be run and in what sequence
- Identify number of workstations needed
- Check out any off-line equipment needs for each application
- Check on forms needed for each application
- Check all data being taken to backup site before leaving and leave inventory profile at home location
- Set up primary vendors for assistance with problems incurred during emergency
- Plan for transportation of any additional items needed at backup site
- Take directions (map) to backup site
- Check for additional magnetic tapes, or optical media if required
- Take copies of system and operational documentation and procedural manuals.

- Ensure that all personnel involved know their tasks
- Notify insurance companies

Testing the disaster recovery plan
in successful contingency planning, it is important to test and evaluate the plan regularly.

Record of plan changes
Keep your plan current, and keep records of changes to your configuration, your applications, and your backup schedules and procedures.

20. Wireless use policy

A wireless use policy is necessary to computer security since there is demand for wireless equipment in every organization today. The wireless use policy may specify that no wireless equipment should be used but this would not be very good since that may cause some to violate the policy. It is best to set conditions and specify equipment that is approved for wireless use in order to minimize security risk associated with wireless.

Overview
This wireless use policy defines the use of wireless devices in the organization and specifies how wireless devices shall be configured when used.

Purpose
This policy is designed to protect the organizational resources against intrusion by those who would use wireless media to penetrate the network.

Scope
This policy applies to all wireless devices in use by the organization or those who connect through a wireless device to any organizational network.

Risk assessment
The use of wireless technology has historically been a serious security risk to organizations. This is because it can be an easy access point to gain access to an organizational network. In addition data sent across it may be readable sometimes even when it is encrypted due to some of the vulnerabilities of the encryption schemes used. Therefore this policy requires a risk assessment any time a new type of wireless device is added to the network. Several items must be assessed including:

- Is this a new technology?
- Does this device use encryption and if so how well tested is the encryption protocol?

- What is the cost of implementing a secure encryption protocol?
- Has this type of device been used on our network before?
- Can this device be configured to only allow authorized users to access it or the network through it?
- How easy will it be for an attacker to fool this device into allowing unauthorized access? What methods may be used?
- What secure authentication schemes are available and what cost or overhead is associated with their implementation and maintenance?
- How practical is wireless use considering the cost, potential loss, and added convenience?

Authentication

The authentication mechanisms of all approved wireless devices to be used must be examined closely. The authentication mechanism should be used to prevent unauthorized entry into the network. One authentication method shall be chosen. The following must be considered.

- How secure is the authentication mechanism to be used?
- How expensive is the authentication mechanism to be used?

Encryption

The encryption mechanisms of all approved wireless devices to be used must be examined closely. The encryption mechanism will be used to protect data from being disclosed as it travels through the air. The following must be considered.

- How secure is the encryption mechanism?
- How sensitive is the data traveling through the wireless device?
- How expensive is the encryption mechanism?

Configuration

The SSID of the wireless device shall be configured in such manner so it does not contain or indicate any information about the organization, its departments, or its personnel including organization name, department name, employee name, employee phone number, email addresses, or product identifiers.

Access points

All wireless access points and wireless devices connected to the organizational network must be registered and approved by the designated IT department representative. All wireless devices are subject to IT department audits and penetration tests without notice.

Authority

The acting CIO or highest level member of IT management shall have final authority over the management and security of wireless devices and wireless networking. This person may delegate these authorities as they see fit. It is strongly recommended that this person has significant experience and training in the IT field along with a

substantial understanding of computer security concepts. This person should be responsible for the operation of the network.

Network separation
This policy requires that parts of the network containing and supporting wireless devices directly (the wireless network) be separated from the part of the network that does not support wireless connections. The part of the network supporting wireless devices or connections shall be considered less trusted than the part of the network that does not. All file servers and internal domain controlling servers shall be separated from the wireless network using a firewall. One or more intrusion detection devices shall monitor the wireless network for signs of intrusion and log events. The type of logged events will be determined by the network administrator.

Allowable wireless use

- Only wireless devices approved by make and model shall be used.
- All wireless devices must be checked for proper configuration by the IT department prior to being placed into service.
- All wireless devices in use must be checked monthly for configuration or setup problems.

Enforcement
Since improper use of wireless technology and wireless communications can open the network to additional sniffing and intrusion attacks, authorized and proper use of wireless technology is critical to the security of the organization and all individuals. Employees that do not adhere to this policy may be subject to disciplinary action up to and including dismissal.

21. Password policy

The StratAgile Information Security Policy requires the use of strictly controlled passwords for accessing Protected Confidential Information (CI) and Internal Information (II). (See StratAgile Information Security Policy for definition of these protected classes of information.) Listed below are the minimum standards that must be implemented in order to ensure the effectiveness of password controls.

Standards for accessing CI, II:

- Users are responsible for complying with the following password standards:
- Passwords must never be shared with another person, unless the person is a designated security manager.
- Every password must, where possible, be changed regularly – (between 45 and 90 days depending on the sensitivity of the information being accessed)
- Passwords must, where possible, have a minimum length of six characters.

- Passwords must never be saved when prompted by any application with the exception of central single sign-on (SSO) systems as approved by the ISO. This feature should be disabled in all applicable systems.
- Passwords must not be programmed into a PC or recorded anywhere that someone may find and use them.
- When creating a password, it is important not to use words that can be found in dictionaries or words that are easily guessed due to their association with the user (i.e. children's names, pets' names, birthdays, etc…). A combination of alpha and numeric characters is more difficult to guess.
- Where possible, system software must enforce the following password standards:
- Passwords routed over a network must be encrypted.
- Passwords must be entered in a non-display field.
- System software must enforce the changing of passwords and the minimum length.
- System software must disable the user identification code when more than three consecutive invalid passwords are given within a 15 minute timeframe. Lockout time must be set at a minimum of 30 minutes.
- System software must maintain a history of previous passwords and prevent their reuse.

22. Risk assessment policy and template

A three stage security and risk analysis in the following tempte needs to be followed for every project and product development.

Step 1: Risk Identification	Step 2: Risk Assessment		Step 3: Risk Management				
List of possible risks	Likelihood H/M/L	Impact H/M/L	What are we already doing about it? (mitigating factors)	What more can we do about it?	Timescale	Person responsible	Reviewed level of risk

Date to be reviewed	
Person/Group responsible for review	

23. Application security policy

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities be remediated prior to production deployment. The purpose of this policy is to define web application security assessments within StratAgile. Web application assessments are performed to identify potential or realized weaknesses because of inadvertent mis-configuration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of StratAgile services available both internally and externally as well as satisfy compliance with any relevant policies in place.

Scope

This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at StratAgile.

All web application security assessments will be performed by delegated security personnel employed StratAgile. All findings are considered confidential and are to be distributed to persons on a “need to know” basis. Distribution of any findings outside of StratAgile is strictly prohibited unless approved by the Head, Infrastructure.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

Application security policy

Applications are subject to security assessments based on the following criteria:

- New or Major Application Release – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.
- Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.
- Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
- Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.
- Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as

such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

- High - Any high-risk issue must be fixed immediately, or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.
- Medium - Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.
- Low - Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

The following security assessment levels shall be established by the InfoSec organization or other designated organization that will be performing the assessments.

- Full - A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of all discovered.
- Quick - A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.
- Targeted - A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

Tools for application security

The current approved web application security assessment tools in use which will be used for testing are:

- Netsparker penetration test
- NeoLoad for load testing
- Google cloud security scanner
- Google page speed test

Other tools and/or techniques may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the Security Engineering team.

Web application protection

If the applications are deployed over web such as a web portal StratAgile will configure necessary security firewalls and coding methods to make the application secure. Few of the security measures across the application are physical separation of database and web servers, opening ports only for necessary IP ranges. On cloud-based applications we also provide configuration of web application firewalls (WAF), antivirus, and dedicated cloud account and VPC.

24. Software development lifecycle (SDLC) policy

The purpose of this policy is to establish a standard expectation for implementation of a Software Development Lifecycle (SDLC) that produces software that is secure, accessible, mobile ready, and compliant with State development standards, policies, and practices. The SDLC must address common business and development phases to be effective across the enterprise, and must address key issues of security, accessibility, mobile device access, and standards compliance. StratAgile employs a spiral model for its software development that consists of the stringent standards of waterfall model and an option to have prototyping and release the products and projects in phases.

Software development projects must address the following areas in a manner consistent with business and development practices. All seven SDLC phases must be addressed and incorporated in a consistent manner. Developers may make necessary adaptations based on the size and complexity of projects. Policy implementation may incorporate standards and guidelines that may be more stringent than the control points or phases identified in this SDLC.

SDLC Phases

- ***Preliminary analysis***: Based upon a stakeholder's initiation request, the objective of this phase is to conduct a preliminary analysis, propose alternative solutions, describe costs and benefits and submit a preliminary plan with recommendations. Every project or task has risks. Cost, time, implementation, security, privacy and regulatory risks may be identified. Risk reduction and mitigation plans are to be considered as part the preliminary analysis of any development effort and management and technical clearance needs to be implemented.
- ***Systems analysis, requirements definition***: Defines project goals into defined functions and operation of the intended application. Analyzes end-user information needs. Address requirements for security, mobility, accessibility, and platform use expectations.
- ***Systems design***: Describes desired features and operations in detail, including screen layouts, business rules, process diagrams, pseudo code and other documentation. Depending upon the size of the project, prototyping is

useful in this stage. Larger complex projects require more definition and more controls.

- ***Development***: Actual development of code, preferably in functional components that can be tested separately, applications must be deployed within a secure hosting environment. Development, testing, and production databases must be physically separated, and all data used in non-production environment must be anonymized by removing the personally identifiable information (PII).
- ***Integration and testing:*** Bring all the pieces together into a testing environment, then checks for errors, bugs and interoperability, accessibility, mobility, performance, standards compliance, and an independent security review such as accessibility testing, environment, integration, system testing, UI testing, unit testing, load testing.
- ***Acceptance, installation, deployment***: The final stage of initial development, where the software is put into production and runs actual business. This is the final checkpoint on architectural compliance, application and hosting security. Development (DEV). Please note acceptance, and production environments must be physically separate instances on different servers.
- ***Maintenance Plan***: What happens during the rest of the software's life: changes (compliance with State Change Control policies), corrections, additions, moves to a different hosting platform, decommissioning, and more.

Document revision history

Version	Date	Author/Editor	Comments
1.0	2013/Aug/10	Ashly Markose	Initial policy document is created
1.1	2014/May/20	Rakesh Vijan	Revision history is added
1.2	2015/Aug/21	Husain Rashid	Incident management updated
1.3	2016/Mar/23	Avish Joseph	Password policy updated
1.4	2016/Jul/02	Avish Joseph	Wireless policy updated
1.5	2016/Nov/20	Avish Joseph	BCP & DR policy created
1.6	2018/Jan/12	Ashly Markose	SDLC policy updated