
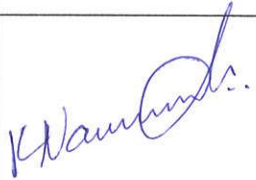
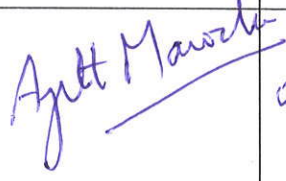


TITLE: INFORMATION SECURITY POLICY**POLICY NUMBER: S/IT/ISMS/ISP/001****DOCUMENT CLASSIFICATION: Confidential****VERSION NUMBER: 003****EFFECTIVE DATE: 04.01.2021****1. Authorized Signatures:**

This Information Security Policy has been reviewed by the following Subject Matter Experts (SME) for its completeness / accuracy and is approved for implementation.

This document is prepared, reviewed and approved by the following personnel.

Responsibility	Name of the Personnel	Signature	Date
Prepared by	Hariharan Subramani Risk and compliance – Senior Manager		25 JAN 2021
Reviewed by	Nandakumar Krishnachar Legal Head		29 JAN 2021
Approved by (CIO)	Ajit Manocha Chief Information Officer		04 FEB 2021

2. Table of contents:

- 1. Authorized Signatures: 1
- 2. Table of contents:..... 2
- 3. Objective: 5
- 4. Scope:..... 5
- 5. Definitions 5
- 6. Information Security Management Policy 8
 - 6.1 Information Security Management (A.5.1.1)..... 8
 - 6.2 Review of Information Security Policy (A.5.1.2) 8
- 7. Organization of Information Security Policy 9
 - 7.1 Internal Organization (A.6.1) 9
 - 7.2 Mobile Devices and Teleworking (A.6.2)..... 10
- 8. Human Resources (HR) Security Policy 11
 - 8.1 Prior to Employment (A.7.1)..... 11
 - 8.2 During Employment (A.7.2) 11
 - 8.3 Termination or change of employment (A.7.3.1)..... 12
- 9. Asset Management Policy 13
 - 9.1 Responsibility for Information Assets (A.8.1)..... 13
 - 9.2 Classification and Handling of Information Assets (A.8.2)..... 13
 - 9.3 Media Handling (A.8.3)..... 15
- 10. Access Control Policy 16
 - 10.1 Business Requirements for Access Control (A.9.1)..... 16
 - 10.2 User Access Management (A.9.2)..... 16
 - 10.3 User Responsibilities (A.9.3) 18
 - 10.4 System Access Control (A.9.4)..... 19
- 11. Cryptography Policy 21

- 11.1 Cryptographic Controls (A.10.1.1)..... 21
- 11.2 Key Management (A.10.1.2)..... 21
- 12. Physical and Environmental Security Policy..... 22
 - 12.1 Secure Areas (A.11.1)..... 22
 - 12.2 Equipment Security (A.11.2) 24
- 13. Operations Management Security Policy 26
 - 13.1 Operational Procedures and Responsibilities (A.12.1)..... 26
 - 13.2 Protection from Malware (A.12.2) 27
 - 13.3 Backup (A.12.3) 27
 - 13.4 Logging and Monitoring (A.12.4)..... 28
 - 13.5 Control of Operational Software (A.12.5) 29
 - 13.6 Technical Vulnerability Management (A.12.6) 29
 - 13.7 Information Systems Audit Considerations (A.12.7) 30
- 14. Communications Security Policy..... 31
 - 14.1 Network Security Management (A.13.1)..... 31
 - 14.2 Information Transfer (A.13.2)..... 32
- 15. System Acquisition, Development and Maintenance Policy..... 34
 - 15.1 Security Requirements of Information Systems (A.14.1)..... 34
 - 15.2 Security in Development and Support Processes (A.14.2) 34
 - 15.3 Test Data (A.14.3)..... 34
- 16. Supplier Relationship Policy 35
 - 16.1 Information Security in Supplier Relationships (A.15.1)..... 35
 - 16.2 Supplier Service Delivery Management (A.15.2) 36
- 17. Information Security Incident Management Policy 37
 - 17.1 Management of Information Security Incidents and Improvements (A.16.1)..... 37
- 18. Business Continuity Management Policy..... 40

- 18.1 Planning Information Security Continuity (A.17.1.1)..... 40
- 18.2 Implementing Information Security Continuity (A.17.1.2)..... 40
- 18.3 Verify, Review and Evaluate Information Security Continuity (A.17.1.3)..... 41
- 18.4 Availability of Information Processing Facilities (A.17.2.1)..... 41
- 19. Information Security Compliance Policy 42
 - 19.1 Compliance with Legal and Contractual Requirements (A.18.1) 42
 - 19.2 Information Security Reviews (A.18.2)..... 43
- 20. Mobile Device Management Policy..... 44
- 21. Acceptable Usage Policy..... 45
- 22. Exceptions 50
- 23. Revision History: 50

3. Objective:

The objectives of Information Security Policy are:

- To provide support and direction on different aspects of information security
- To act as a guiding factor in developing relevant policies, procedures, templates, guidelines etc. related to information security

4. Scope:

The policies included in this document apply to all Syngene employees including third party contract employees. These policies are applicable to all Information Systems (IS) environments operated by Syngene. The term “IS environment” defines the total environment and includes, but is not limited to, all electronic and hard copy documentation, physical and logical controls, personnel, hardware (e.g. servers, desktops, lab instruments, etc.), software, and information.

5. Definitions

Terms	Definition
A.x.x.x	Indicates the respective ISO 27001:2013 controls
ISC	Information Security Committee
ISRC	Information Security Risk and Compliance
Availability	Availability is a characteristic that applies to assets. An asset is available if it is accessible and usable when needed by an authorized entity. Assets include things like information, systems, facilities, networks, and computers. All of these assets shall be available to authorized entities when they need to access or use them.
Confidentiality	Confidentiality is a characteristic that applies to information. To protect and preserve the confidentiality of information means to ensure that it is not made available or disclosed to unauthorized entities. In this context, entities include both individuals and processes.
Integrity	To preserve the integrity of information means to protect the accuracy and completeness of information and the methods that are used to process and manage it.
Information Asset	Information Asset is a definable piece of information, stored in any manner which is recognized as 'valuable' to the organization.
Information Security	Information Security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Information Security Management System (ISMS)	Information Security Management System (ISMS) refers to a set of policies and processes established by management to assess the security requirements, develop and implement controls, evaluate effectiveness of controls and implement improvements following a continuous improvement process.
Information Security Incident	An Information Security incident is made up of one or more unwanted or unexpected Information Security events that could very likely compromise the security of your information and weaken or impair your business operations.
Risk	Combination of the probability of an unwanted event and its consequence.
Threat	A threat is a potential event. When a threat turns into an actual event, it may cause an unwanted incident. It is unwanted because the incident may harm an organization or system.
Vulnerability	Vulnerability is a weakness in an information asset or group of information assets. An information asset's weakness could allow it to be exploited and harmed by one or more threats.
Cryptography	Cryptography is the transformation of plain data into encoded data by the use of encryption and the decoding of encoded data by decryption. Cryptography relies on two basic components: a cryptographic algorithm and a cryptographic key.
Cryptographic Algorithm	A cryptographic algorithm is a mathematical function used for encryption and decryption.
Encryption Key	The encryption key is a piece of data used in conjunction with a cryptographic algorithm. The key acts as a lock to the encryption process. Knowledge of the appropriate key is required in order to encrypt or decrypt the data. The encryption key is often referred to as the keying material. Keys used in asymmetric cryptography are normally referred to as 'private' and 'public' keys, whilst those used in symmetric cryptography are referred to as 'secret' keys or 'shared secrets'
Key Length	The key length describes the amount of data required for the cryptographic key. In the case of cryptographic keys for computer-based algorithms this is normally expressed as a number of bits. Some algorithms require a fixed key length, while others except variable key lengths. Typically, the larger the key the more difficult a well-written algorithm becomes to break. It is important to note that it is not normally possible to directly compare the comparative strength of different algorithms based on key length alone.

Business Continuity	Ability of an organization to maintain essential functions during as well as after a disaster has occurred
Peer-to-Peer (P2P) Software	Peer-to-Peer (P2P) software is used to share copyrighted information across the Internet. If use of such software is allowed, copyrighted and/ or other confidential material could be accessed or shared without the knowledge of the Information Security function.
Proxy Server	A Proxy Server is a security system used to protect internal users accessing the Internet from external threats.
Network Scanning or Hacking Tools	Software programs used for intercepting network communications or interrogating computer systems on the network or the Internet. Such tools could be used by unauthorized individuals to gain access to sensitive information and/ or launch attacks on the company network and systems.

6. Information Security Management Policy

6.1 Information Security Management (A.5.1.1)

- The main goal of Information Security at Syngene is to ensure:
 - Confidentiality of information – sensitive Syngene information shall only be accessible to those authorized to access such information
 - Integrity of information – business critical Syngene information shall remain accurate, error free and without omissions
 - Availability of information – authorized users shall have access to critical business information when required
- The objective of the Information Security Management System is:
 - To ensure information assets and technologies are adequately protected
 - To identify, develop, implement and maintain processes across the organization to reduce information and information technology risk
 - To respond to incident, establish appropriate standards and controls, manage security technologies and direct the establishment and implementation of policies and procedures
- To meet the above mentioned Information Security objectives Syngene shall ensure the following:
 - Controls shall be established and implemented to meet the objectives;
 - Internal review and external review shall be performed on a periodic basis; and
 - Implement improvements following a continuous improvement process
- The Information Security Management System (ISMS) shall be implemented through a set of policies, procedures and standards for all full-time employees and sub-contractors
- All full-time employees and sub-contractors shall be responsible for complying with Information Security policies at Syngene
- Any breach of Information Security, either suspected or actual, shall be promptly reported to the Lead - ISRC.
- Any violations of the Information Security policies shall be considered a serious offense and disciplinary actions may be pursued in-line with the Syngene's Disciplinary Policy.

6.2 Review of Information Security Policy (A.5.1.2)

- Syngene's Information Security Policy shall be reviewed annually to ensure their continuing suitability, adequacy and effectiveness
- Significant changes to the organizational environment such as business circumstances, contractual, regulatory or legal conditions, or to the technical environment shall trigger ad-hoc security policy reviews
- Recommendations provided by relevant authorities and/or other entities, both within and outside the organization, shall be part of the security policy review agenda.

7. Organization of Information Security Policy

7.1 Internal Organization (A.6.1)

Information Security Roles and Responsibilities (A.6.1.1)

- Information security roles and responsibilities shall be incorporated in the job description of each employee and service provider.
- These roles and responsibilities shall include general responsibilities applicable to all users at Syngene as well as specific responsibilities based on the criticality and sensitivity of information and information processing systems expected to be handled by the user.
- All Syngene employees and service providers' supplier shall be informed about their roles and responsibilities for information security prior to employment.
- Security roles and responsibilities of the suppliers shall be included in the agreement between Syngene and suppliers.

Segregation of Duties (A.6.1.2)

- Segregation shall be maintained between conflicting duties to reduce the risk of accidental or deliberate system misuse.
- The initiation of an event shall be separated from its authorization, monitoring or audit.
- Where segregation of duties is not possible, an authorization shall be sought, and compensating controls shall be implemented to avoid any negligent or fraudulent activities.

Contact with authorities (A.6.1.3)

- Syngene shall maintain a list of emergency contact details of all the relevant public service authorities like police, fire department, hospitals etc.
- Syngene shall immediately contact appropriate authorities in case of an incident and address the same in a timely manner.

Contact with Special Interest Groups (A.6.1.4)

- Syngene shall subscribe to information security forums, newsletters, vendor specific security sites so as to be abreast of the latest information security related news and best practices.

Information Security in Project Management (A.6.1.5)

- Information security shall be integrated into Syngene's project management method(s) to ensure that information security risks are identified and addressed as part of a project.
- Syngene shall implement this control for all kinds of projects irrespective of its nature.
- Information Security objectives shall be included in project objectives.
- An information security risk assessment shall be conducted at an early stage of the project (where applicable) to identify necessary controls.

- Information security shall be a part of and addressed in all phases of the project management lifecycle.
- Information security implications shall be addressed and reviewed regularly for all projects.
- Responsibilities for information security shall be defined and allocated to specified roles defined in the project management methods.

7.2 Mobile Devices and Teleworking (A.6.2)

Mobile Device Policy (A.6.2.1)

- Use of mobile computing devices such as laptops, PDAs, smartphones etc. shall be authorized.
- Every mobile computing and communication device shall have a designated owner.
- Risks associated with the use of mobile computing and communication devices shall be identified.
- Security measures shall be configured on the mobile computing and communication devices to ensure protection of information contained therein.

Teleworking (A.6.2.2)

- Any regular and recurring telework arrangement shall be granted only after authorization.
- Adequate teleworking security measures shall be established and implemented.

8. Human Resources (HR) Security Policy

8.1 Prior to Employment (A.7.1)

Screening (A.7.1.1.)

- Background checks shall be performed on all candidates for employment in accordance with relevant laws, regulations and ethics.

Terms and Conditions of employment (A.7.1.2)

- The terms and conditions of employment shall include the employee's responsibilities for information security and related obligations, both during and after employment
- All Syngene information asset users, including contractors, shall be required to sign and agree to comply with their employment terms and conditions, as well as Syngene's confidentiality/non-disclosure agreement, before being granted access to information
- All Syngene information asset users, including contractors, shall be required to sign and agree to comply with Syngene's acceptable usage policy, confidentiality agreement and clear desk and clear screen policy

8.2 During Employment (A.7.2)

Management Responsibilities (A.7.2.1)

- All Syngene information asset users shall be properly briefed regarding their roles and responsibilities with respect to information security, and the acceptable usage of Syngene's information assets and processing facilities
- All Syngene employees, contractors shall be required to apply security in accordance with Syngene's established policies and procedures
- Security responsibilities shall be included in the performance evaluation of the personnel assigned significant security roles

Information Security Awareness, Education and Training (A.7.2.2)

- Syngene requires its employees and contractors to complete an Information Security eLearning Training course annually. The objective of this course is to raise Syngene employees' and contractors' information security awareness and familiarizes them with key general Information security policies and standards
- New employees shall complete the training course as part of their induction program within 30 days after they have joined and received access to Syngene systems
- The Information security team shall develop and deploy a formal, documented security awareness and training program that addresses actual cyber security related risks and topics. The program should also consider specific audiences in the business who are handling sensitive information and are more likely targeted by external cyber attackers. The program shall be revised annually

- Training records must be documented individually in order to ensure it can be audited, tracked, and reported on a regular basis. Training records must be retained until the end of the next financial year
- At a minimum, the annual security awareness program shall include topics as per the defined procedures.

Disciplinary Process (A.7.2.3)

- Syngene shall ensure a comprehensive Disciplinary Process is in place to handle all kind of security breach and cases of misconduct.

8.3 Termination or change of employment (A.7.3.1)

- The responsibilities for performing employment termination and/or change of employment shall be defined, documented and clearly communicated
- A formal termination process shall be defined and implemented. Such process shall include considerations such as exit interviews, access revocation, return of assets, and review of termination checklists
- Employment contracts / vendor agreements shall include the duties and responsibilities that shall be valid after the termination of such contract or agreement
- Upon termination, Syngene users, including contractors shall return / hand-over, all organization's information assets under their purview. Such assets shall be returned / handed over to Syngene in accordance with the defined and approved termination procedures
- In the case of change of employment, the access rights and/or privileges granted to employees and contractors shall be formally reviewed and accordingly adjusted

9. Asset Management Policy

9.1 Responsibility for Information Assets (A.8.1)

Inventory of Assets (A.8.1.1)

- Responsibilities shall be defined to create and maintain asset inventories at Syngene.
- Inventories of all assets shall be maintained for each function in scope of ISMS
- The Information Asset Inventory shall contain the following information as a minimum:
 - Asset identification
 - Asset description
 - Asset location
 - Asset Owner
 - Asset classification
 - Validity of the classification

Ownership of Assets (A.8.1.2)

- All Information assets shall have a designated owner.
- The owner of the asset shall be responsible for controlling the access and use of the asset.

Acceptable Use of Assets (A.8.1.3)

- Syngene shall identify, document and implement the rules for acceptable use of information assets associated with the information processing facilities

Return of Assets (A.8.1.4)

- Upon termination, Syngene users, including sub-contractors shall return / hand-over, all organization's information assets under their purview. Such assets shall be returned / handed over to Syngene in accordance with the defined and approved termination procedures.

9.2 Classification and Handling of Information Assets (A.8.2)

Classification of Information (A.8.2.1)

- All Syngene information shall be classified by the asset owners based on the confidentiality requirements of the information under the following four categories:
 - **Restricted** - Most sensitive business information that is intended strictly for named individuals such as merger and acquisition documents, information security strategy and corporate level strategic plans.
 - **Confidential** - Information that is considered private and can be accessed only by a limited number of personnel such as human resources data, source code and vendor contracts.

- **Internal** - Information that is meant to be disseminated within the organization or a section of the organization such as company telephone directory, new employee training materials such as newsletters.
- **Public** - Information that is available to the general public and intended for distribution outside the organization such as product and service brochures, advertisements and financial statements.
- The classification level shall take into consideration the information's legal requirements, sensitivity and criticality to the organization.
- All unclassified information shall by default be treated as "Public".
- All information shall be periodically reviewed and reclassified, if required by respective asset owners.
- On reclassification, all known users of the information shall be kept informed.

Labelling of information (A.8.2.2)

- All classified information shall be prominently labelled to ensure that every user of the information can clearly identify the classification level.
- Access restrictions shall be implemented to support the protection requirements of the assets based on its level of classification.
- Disposal of an asset shall be done securely as per the classification level and only after obtaining approval from the respective asset owner.
- Information classification labels shall appear on all the removable media containing information such as hard copies, floppy disks, CD's etc.

Handling of Assets (A.8.2.3)

- Every user shall create, process, store, transmit and declassify any Syngene classified information as per the handling requirements of the respective classification level.
- Procedure for handling assets shall be developed and implemented in accordance with Syngene's information classification scheme and shall cover asset handling, processing, storing and communicating information consistent with its classification.
- A formal record of the authorized recipients of assets shall be maintained.
- IT assets shall be stored in accordance with manufacturers' specifications.
- All copies of media shall be clearly marked for the attention of the authorized recipient.
- All media shall be handled according to the classification level of the information contained therein. Access to media shall be provided to authorized persons only
- All system documentation shall be identified, recorded and maintained securely with limited access to only authorized persons. System documentation held on a public network shall be protected from unauthorized modification.

9.3 Media Handling (A.8.3)

Management of Removable Media (A.8.3.1)

- There shall be controls in place for the management of removal media
- The guidelines for the management of removable media shall be followed as per the standard and the procedures defined:
 - If no longer required, the contents of any removable media that are to be removed from Syngene shall be made unrecoverable;
 - Authorization must be required for media removed from Syngene and a record of such removals shall be kept in order to maintain an audit trail;
 - Media shall be stored in a safe, secure environment, in accordance with manufacturer's specifications;
 - Information stored on media that needs to be available longer than the media lifetime shall be stored elsewhere to avoid information loss due to media deterioration;
 - Registration of removable media shall be considered to limit the opportunity for data loss; and
 - Removable media drives shall only be enabled if there is a business reason for doing so.

Disposal of Media (A.8.3.2)

- Media and equipment shall be securely disposed when no longer required. The IT team is responsible for backing up and sanitizing Syngene related data from any to-be-disposed asset (wherever applicable), as well as the removal of tags and/or identifying labels
- Acceptable methods for the disposal of assets shall be documented

Physical Media Transfer (A.8.3.3)

- Media containing information shall be protected against unauthorized access, misuse, or corruption during transportation

10. Access Control Policy

10.1 Business Requirements for Access Control (A.9.1)

Access Control Policy (A.9.1.1)

- The provision, change, and revocation of user access rights and associated privileges shall be controlled and monitored. Procedures shall be established to ensure that this is done in accordance with this Access Control Policy.
- Procedures to authorize access to Syngene information processing facilities shall be defined and documented. Access shall not be granted until the authorization process has been completed.
- A formal record shall be maintained and be available for examination of all users registered to use Syngene information system or information processing facility. This may be maintained either automatically by the administration of the information processing facility or manually. Where the records are maintained within an information system, functionality shall be available to provide reports to the designated business process owners, providing details of registered users and their access rights.
- Access to Syngene information processing facilities and Syngene official information shall be authorized and approved with proper business justification. Minimum level of privilege/ access (least privileges) shall be given as required to perform their respective job responsibilities.

Access to Network and Network Services (A.9.1.2)

- Users shall only be provided with access to the network and network services that they have been specifically authorized to use.
- This policy shall cover:
 - authorization procedures for determining who is allowed to access which networks and networked services;
 - management controls and procedures to protect access to network connections and network services;
 - the means used to access networks and network services (e.g. use of VPN or wireless network);
 - ensure authentication requirements for accessing various network services;
 - Monitoring the use of network services.
- Formal procedures shall be followed for providing access to the Syngene network and network services.

10.2 User Access Management (A.9.2)

User Registration and de-registration (A.9.2.1)

- A formal user registration procedure shall be documented and followed for granting or modifying access to Syngene information and information processing systems.

- A formal user de-registration procedure shall be documented and followed for revoking access to Syngene information and information processing systems.
- Access privileges shall be revoked on the day an employee or a supplier leaves (by Resignation, Involuntary Termination, movement to other office location, etc.) the organization.
- Ensure that redundant User ID shall not be issue to other users.

User access provisioning (A.9.2.2)

- Formal user access provisioning process shall be implemented by Syngene to assign or revoke access rights for all user types to all systems and services.
- The provisioning process for assigning or revoking access rights granted to user IDs shall include:
 - Obtain authorization from the owner of the information system or service for the use of the information system or service. A separate approval for access rights from management may also be appropriate
 - Verify that the level of access granted is appropriate to the access policies and is consistent with other requirements such as segregation of duties;
 - Ensure that access rights are not activated (e.g. by service providers) before authorization procedures are completed;
 - Maintain a central record of access rights granted to a user ID to access information systems and services;
 - Adapt access rights of users who have changed roles or jobs and immediately remove or block access rights of users who have left the organization;
 - Periodically review access rights with owners of the information systems or services

Management of privilege access rights (A.9.2.3)

- Privileges associated with each type of operating system, business applications, databases and network elements shall be identified and documented.
- The allocation and use of privileges shall be restricted and tightly controlled.
- Privileges shall be allocated to individuals on a "need-to-use" basis and on an "event-by-event" basis i.e. the minimum requirement for their functional role only when needed.
- The default-privileged accounts, on information processing systems, shall be renamed, wherever feasible.
- Use of privileged IDs shall be logged and such logs shall be reviewed regularly.
- Privileges shall be assigned to a different user ID and not to those used for normal business use.

Management of secret authentication information user (A.9.2.4)

- User shall sign the statement to keep personnel secret authentication information confidential and to keep group (i.e. shared) secret authentication information solely within the members of the group.
- User shall be provided initially with secure temporary secret authentication information, which they are forced to change on first use.
- Procedures shall be established to verify the identity of a user prior to providing new, replacement or temporary secret authentication information.
- Temporary secret authentication information shall be given to users in a secure manner; the use of external parties or unprotected (clear text) electronic mail messages shall be avoided.
- Temporary secret authentication information shall be unique to an individual and shall not be guessable.
- Users shall acknowledge receipt of secret authentication information.

Review of User Access Rights (A.9.2.5)

- Access rights of all the users on Syngene information processing systems shall be reviewed on a periodic basis to ensure that access provided is appropriate as per job functions.
- User ID's that is inactive for more than 60 days shall be disabled.
- All user activities on Syngene information processing systems shall be logged and monitored for adherence to security policies.

Removal or adjustment of access rights (A.9.2.6)

- The access to all applications and information processing systems shall be disabled or removed immediately after the termination of employment, contracts and agreements.
- Change of employment or contractual status shall include removal of rights associated with prior rules and responsibilities and the creation of rights appropriate to the new rules and responsibilities.
- Access rights to Syngene employees and supplier shall be removed or reduced according to following factors:
 - The current responsibility of employees of suppliers or other users;
 - Criticality of assets that are currently accessible.
 - Nature of termination or changing responsibilities of employees, supplier etc.

10.3 User Responsibilities (A.9.3)**Use of secret authentication information (A.9.3.1)**

- Adequate controls shall be implemented to force strong password parameters as per Syngene password policy.

- Passwords for the network, operating systems, applications and databases shall be governed by the password policy.
- All Syngene employees, suppliers shall follow Syngene's policies in the use of secret authentication information.
- Mandatory Passwords Standards (applicable for all systems and applications):
 - Minimum password length = 8 characters
 - Complexity = passwords must contain at least 3 out of the following requirements:
 - one upper case alpha character
 - one lower case alpha character
 - one number
 - One special character (i.e. punctuation characters that are present on standard keyboard – e.g. ! %, &, \$)
- User ID should be locked after maximum 10 failed attempts at log in
- Systems must lock out / time out after 05 minutes of inactivity
- Password expiry of 90 days for all domain-based logons and systems with sensitive data (i.e. Operating systems and Financially Critical Applications) should be implemented.
- All Syngene employee shall be advised to:
 - Keep secret authentication information confidential, ensuring that it will not accessible to any other parties
 - Avoid keeping records of secret authentication information which may cause loss of CIA (Confidentiality, Integrity, Availability), unless this can be stored securely, and the method of storing has been approved by the IS department.
 - If there is any indication of possible compromise, then change the secret authentication information.
 - If your using password as secret authentication information, then follow password policy design by Syngene Information Security department

10.4 System Access Control (A.9.4)

Information Access Restriction (A.9.4.1)

- Access to information and application system shall be restricted in accordance with the defined Access Control Policy.
- Access given not according to the Access Control Policy shall be supported with a valid justification and approval by the data owners.

Secure Log-on Procedures (A.9.4.2)

- Logon procedures for Syngene Information Systems and services shall provide a mechanism to detect multiple unsuccessful attempts at logging on.

- The logon process shall invoke a protection mechanism if the authentication process is repeated unsuccessfully more than a specified number of times for the same user. The number of consecutive unsuccessful attempts by the same user is defined in the “Password Management” procedure. The protection mechanism shall:
 - Reject further logon attempts;
 - Temporarily disable the user’s access;
 - Record the event for audit; and
 - Raise an alert.
- An advisory warning message shall be displayed to the user prior to initiating an information system or service logon procedure.
- Systems shall display a warning message before the user is allowed to logon. (The message shall inform the person attempting to access the system that the use of the information system resource is governed by a security policy, contravention of which may lead to internal disciplinary action or legal proceedings).

Password Management System (A.9.4.3)

- Any operating system and application installed at Syngene shall be configured in compliance with Syngene Password Policy.

Use of Privileged Utility Program (A.9.4.4)

- Access to system utilities shall be granted only to authorize personnel to carry out administrative or business required activities.
- Any third-party using system utilities shall be approved by Syngene and activities carried out shall be logged and reviewed as per the procedure.

Access Control to Program Source Code (A.9.4.5)

- Access to source code and object libraries shall be appropriately restricted and controlled.
- Where possible, program source libraries shall not be held in operational systems.
- Syngene shall follow appropriate version management processes to ensure integrity of program source codes.

11. Cryptography Policy

11.1 Cryptographic Controls (A.10.1.1)

- Based on the business need, cryptographic controls shall be identified and implemented to provide appropriate level of protection to Syngene's information and Information Systems.
- The need for cryptographic controls shall be identified based on the information's classification level.
- The encryption algorithms suitable for Syngene's business and information security needs shall be identified and a record of all approved encryption software and algorithms, along with the acceptable key length for each shall be maintained.
- Only approved encryption software and cryptographic products shall be used for Syngene information and information processing systems.
- Digital signatures shall be used, where required, for ensuring message authentication, integrity and non-repudiation.
- Cryptographic controls used shall be reviewed at least annually to assess their effectiveness taking into consideration the developments in industry standards, changes in business operations and any compromise of information occurred, if any.
Pass phrases used for applying cryptographic controls shall be protected from unauthorized access and disclosure.

11.2 Key Management (A.10.1.2)

- The owners and custodians for the encryption keys shall be clearly defined for all cryptographic software used by Syngene. Key management activities shall be logged and monitored.
- Roles and responsibilities shall be designed for secure generation, storage, distribution, usage, change, revocation, destruction, recycling and archival of encryption keys.
- Access to encryption software and encryption keys shall be restricted and shall be made available only to authorized personnel.
- Equipment used to generate, store and archive keys shall be physically protected.
- The minimum length of the encryption keys shall be defined in accordance with contractual requirements, applicable legal regulations, national restrictions (for import, export and utilization of cryptographic hardware and software) and license requirements. Encryption keys shall be changed periodically or on disclosure.
- The encryption keys shall be stored and archived securely to minimize the chances of their unauthorized access and misuse. Only secure communication channels shall be used for distribution of encryption keys and the keys shall never be transmitted in an un-encrypted format.
- Procedures shall be defined for verifying credentials of requesters before sharing keys and for ascertaining the authenticity of the counterparty before establishing a trusted path.

12. Physical and Environmental Security Policy

12.1 Secure Areas (A.11.1)

Physical Security Perimeter (A.11.1.1)

- Physical security controls shall be managed and maintained by Engineering and Maintenance (EAM) Team, while the Environmental security controls shall be maintained and managed by the Environmental Health Safety and Security (EHSS) Team.
- Perimeter security controls such as walls, card-controlled entry gates and/or manned reception desks shall be implemented to protect areas that contain information and information processing facilities.
- All external doors and windows shall be suitably constructed and protected against unauthorized access, with control mechanisms such as bars, alarms and/or locks.
- The extent of physical protection provided to information systems and information processing facilities shall be subject to a security risk assessment, and in accordance with the asset classification standards and guidelines.
- Sensitive and/or critical information processing facilities shall be identified and appropriately segregated into protected zones.
- Doors and windows of unattended information processing facilities shall be locked and periodically reviewed.

Physical Entry Controls (A.11.1.2)

- Access to all critical information processing facilities shall be granted in accordance with the “Syngene Physical & Environmental Security Procedure”. Such access shall be logged and securely maintained by EAM team and shall be regularly reviewed by respective facility owners.
- Secure areas shall be protected by appropriate physical entry controls, to ensure that only authorized personnel are permitted to access such areas.
- Access to secure areas shall only be granted in accordance with the “Syngene Physical & Environmental Security Procedure”.
- Access to all sensitive and/or critical information processing facilities such as data centres and computer rooms shall be logged / recorded.
- Access logs shall be securely maintained, and access to such logs shall be restricted and controlled.
- Access logs shall be regularly reviewed to detect unauthorized access or inappropriate access rights.
- Physical access rights shall be regularly reviewed to ensure that such rights are maintained in accordance with the current access requirements.
- Upon transfer or termination, physical access rights granted to users shall be promptly revoked / amended in accordance with the employee termination or transfer procedures.

Securing Office, Rooms and Facilities (A.11.1.3)

- Access to all office, rooms and facilities shall be granted in accordance with the “Syngene Physical & Environmental Security Procedure”. All access shall be monitored by the respective facility owners.
- All information processing facilities such as data centre, computer rooms, telecommunication closets / cabinets, etc. shall be designed, constructed and sited to avoid unauthorized or unnecessary access.
- Maps, floor plans and other documents that describe the location of sensitive and/or critical information processing facilities shall not be readily available or accessible to the public.
- Syngene’ offices, rooms and facilities shall be designed and constructed in accordance with all applicable health and safety regulations, standards and guidelines.

Protecting against External and Environmental Threats (A.11.1.4)

- Syngene shall ensure that sensitive and/or critical information processing facilities are appropriately equipped and maintained with security controls to safeguard the information contained within the facility against man-made or environmental threats.
- Syngene shall conduct regular awareness and training programs, for employees on how to identify, respond to and manage external and environmental threats.
- Syngene shall conduct periodic fire and safety drills and evaluate employee participation and response.

Working in Secure Areas (A.11.1.5)

- Appropriate physical protection procedures and guidelines for working in secure areas shall be defined, documented and implemented.
- All work performed in secure areas shall be authorized and supervised.
- Unless specifically authorized, personal electronic devices such as, laptops and USB devices shall not be permitted into restricted information processing facilities.

Delivery & Loading Areas (A.11.1.6)

- Delivery and loading areas, as well as other publicly accessible areas shall be appropriately isolated from information assets and information processing facilities.
- External agencies’ access such as courier and delivery services shall be restricted to designated delivery/ collection points.
- All incoming and outgoing items, packages and/or materials shall be registered and inspected by the EAM team.

12.2 Equipment Security (A.11.2)

Equipment Siting & Protection (A.11.2.1)

- Equipment shall be protected from security threats and environmental threats.
- Adequate air conditioning equipment shall be installed to ensure the information assets are protected from environment threats.
- Supporting equipment such as photocopiers, printing devices and fax machines shall be protected from unauthorized physical access.
- Consumption of eatables and beverages inside Network rooms / Data centre shall be prohibited.
- Storing of flammable objects within the Network rooms / Data centre shall be also prohibited.

Supporting Utilities (A.11.2.2)

- Adequate control measures shall be in place to protect the information assets from power failures and other disruptions caused due to failures in water supply and waste disposal.
- Sufficient supporting utilities for fall-back procedures such as UPS, DG Sets and fuel supply shall be ensured.

Cabling Security (A.11.2.3)

- Power and network / telecommunications cabling carrying data or supporting information services shall be protected from interception or damage. They shall also be protected to prevent unauthorized access to data transmissions via unauthorized tapping or disruption.

Equipment Maintenance (A.11.2.4)

- Equipment shall be correctly maintained to ensure its continuous availability and integrity.
- Only authorized maintenance personnel shall repair and service the equipment.
- Records shall be maintained of all suspected or actual faults, and of all preventive maintenance.
- Before putting equipment back into operation after its maintenance, it shall be inspected to ensure that equipment has not been tampered with and shall not be affected by viruses or malfunctions.
- All maintenance requirements imposed by insurance policies shall be complied with.

Removal of Assets (A.11.2.5)

- Equipment, information or software shall not be taken off-site without prior authorization. Such authorization shall be in accordance with Syngene' formal authorization and asset handling procedures.

- The off-site removal of equipment, information, software, materials or supplies shall be inspected and recorded. Such removal records shall be maintained and periodically reviewed.
- Removal records shall include items removed on a temporary basis and items removed for repairs.
- Physical asset verification checks shall be periodically performed, to detect unauthorized removal of property from Syngene premises.

Security of Equipment and Assets Off-premises (A.11.2.6)

- Risks to equipment and assets used to support business activities from off-site locations such as servers, personal computers, organizers, mobile phones, smart cards, paper, USB devices or other storage devices, shall be identified and documented.
- Suitable security safeguards such as encryption, hashing / message digests, password protection or physical access controls, shall be identified and implemented to mitigate / reduce the identified risks.

Secure Disposal or Re-use of Equipment (A.11.2.7)

- Any equipment that contains information shall be sanitized before reuse or disposal as per the “Syngene Media Handling & Disposal Procedure”.
- All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

Unattended User Equipment (A.11.2.8)

- Equipment such as personal computers, servers, terminals and other devices shall be protected from unauthorized use and/or access when unattended.
- Appropriate security measures such as password protected screen savers and/or screen or key locks, automated termination of active sessions shall be adopted to protect the unattended equipment.

13. Operations Management Security Policy

13.1 Operational Procedures and Responsibilities (A.12.1)

Documented Operating Procedures (A.12.1.1)

- Syngene shall identify important departments within Syngene operations and document operational procedures with responsibilities for each of them.
- Operating procedures shall be treated as formal documents and creation, modification/changes and removal shall be reviewed and approved by the ISC.
- The documented operating procedures shall be readily available and communicated to those employees whose job function requires the knowledge of said procedures.
- ISC shall review operating procedure on a yearly basis or as and when required in the event of a change to the Syngene policies, legal and regulatory environment, operating environment, technology, organizational processes, roles and responsibilities.

Change Management and Release Management (A.12.1.2)

- Syngene infrastructure availability is critical to the effective operation of Syngene. It is essential to carefully manage changes to the IT infrastructure and applications.
- A change requires serious forethought, impact analysis, authorization, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the availability and reliability of Syngene infrastructure and applications.
- Following is a non-exhaustive list of change sources that this policy shall apply for;
 - Periodic maintenance of infrastructure;
 - User requests;
 - Hardware and/or software upgrades including instrument application software;
 - Acquisition of new hardware and/or software;
 - Changes and/or modifications to the infrastructure and applications;
 - Environmental changes (such as changes to the electrical system as per a requirement of a planned infrastructure change);
 - Operations schedule changes; and
 - Application of patches to infrastructure and applications.
- The Change Advisory Board (CAB) shall be responsible to meet on regular basis to discuss completed, planned and rejected changes. All changes shall follow the approved change and release management procedure for infrastructure and applications and submitted for the CAB review and authorization. CAB shall have the following responsibilities: -
 - Meet regularly to review all requests for change with requestors;
 - Communicate with all stakeholders', critical information about how a given change may impact the current infrastructure or setup and the risk of the change against not carrying out the change;

- Assess the urgency and priority of the proposed change;
- Ensure that adequate testing has been conducted;
- Ensure that testing and approval criteria has been established before implementing the change;
- Ensure that proper fall-back procedures including procedures and responsibilities for aborting and recovering from unsuccessful changes are documented before applying the change;
- Ensure that approved Change and Release Management Procedures are used when carrying out and implementing a change.

Capacity Management (A.12.1.3)

- Syngene shall follow the Performance, Capacity and Availability management procedure to ensure required system performance and availability of resources.
- These procedures shall address resource planning, capacity monitoring, systems tuning and resources projections to meet future demands.
- The use of resources shall be appropriately monitored and tuned in accordance with the documented procedure.

Separation of Development, Testing and Operational Environments (A.12.1.4)

- Production and non-production environments shall be appropriately separated from each other whenever possible.
- Access to the development, testing, quality assurance/ staging and production environments shall be appropriately restricted to prevent intentional or unintentional errors and misuse of systems.

13.2 Protection from Malware (A.12.2)

Control against Malware (A.12.2.1)

- Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

13.3 Backup (A.12.3)

Information Backup (A.12.3.1)

Back-up and Restoration

- In order to facilitate normal and continued business operations, all sensitive information and information system shall be backed up on a regular basis to on-line and off-line storage. However, the information owner and business application owner are required to inform the Backup team on their specific business backup requirements.

- The backup and restoration procedure shall provide the details and frequency of the backup schedule for each business application in-line with the classification of the application and the information it supports. It shall also specify the type of backups required (full, partial, incremental, differential, real-time) at each point in the backup schedule.
- When new systems are commissioned, the backup schedules shall be updated to include these new systems.

Back-up Verification and Testing

- Backup restoration shall be tested in accordance with a formal schedule to ensure that the organization's data availability requirements can be met.
- Backup and restoration testing shall be controlled and supervised.

Backup Storage and Retention

- Back-up media shall be stored and maintained at suitable and secure off-site locations as per Syngene back-up procedures.
- Retention period of the backup shall be in line with the business requirements specified in the backup procedure.
- Back-up media movements shall be logged and regularly reviewed.
- Back-up media shall be stored, clearly labelled and handled in accordance with Syngene media handling procedures to ensure ease of identification and access.

13.4 Logging and Monitoring (A.12.4)

Event Logging (A.12.4.1)

- Syngene shall ensure that following logs are recorded on all critical infrastructure devices including but not limited to servers, applications and software: -
 - Logs of all user activities;
 - Logs of all administrative activities;
 - Exceptions and errors; and
 - Attempts to bypass security.
- Any critical exceptions recorded in the log records shall be reported as Information Security incidents and “Syngene Incident Management procedure” shall be followed.

Protection of Log Information (A.12.4.2)

- Event logs shall be securely maintained so as to provide support for investigations of incidents.
- Logging facilities and log information shall be protected against tampering and unauthorized access.

Administrator and Operator Logs (A.12.4.3)

- System administrator and system operator activities shall be logged for all critical IT infrastructures managed internally or by a third party.
- Infrastructure Manager shall review all the system administrator logs on a periodic basis and any exceptions shall be logged as an Information Security incident.
- Administrator and operator logs shall be recorded and stored in a separate media which shall be inaccessible by the system administrator or the operator.

Clock Synchronization (A.12.4.4)

- Clocks of all information processing systems within Syngene should be synchronized with the Domain Controller.

13.5 Control of Operational Software (A.12.5)**Installation of Software on Operational Systems (A.12.5.1)**

- Any changes to the operational software shall follow the “Change and Release Management Procedure.
- Updates to operational software, applications and program libraries shall only be performed by appropriately trained personnel following management authorization.
- Operational systems shall only hold approved executable code and not development code or compilers.
- Applications and operating system software shall only be implemented after extensive and successful testing; the tests may include tests on usability, security, effects on other systems and user-friendliness and shall be carried out on separate systems (test environment).
- A roll-back strategy where applicable shall be in place prior to implementing changes to production environment.
- An audit log shall be maintained of all updates.

13.6 Technical Vulnerability Management (A.12.6)**Management of Technical Vulnerabilities (A.12.6.1)**

- Syngene shall follow the “Syngene Vulnerability Management procedure” for technical vulnerability assessment and management.
- Timely information about technical vulnerabilities of Information Systems shall be obtained.
- Syngene’s exposure to such vulnerabilities shall be evaluated and appropriate countermeasures shall be defined and implemented in a timely manner to address the associated risks.

Restrictions on Software Installation (A.12.6.2)

Syngene shall identify the types of software installations to be permitted (e.g. updates and security patches to existing software) and the ones to be prohibited.

13.7 Information Systems Audit Considerations (A.12.7)**Information Systems Audit Controls (A.12.7.1)**

- Audits of operational Information Systems shall be planned and performed at periodic intervals with the agreement of the Information Systems' owner so as to minimize the risk of disruption to business processes.
- Audits shall be limited to read-only access to data. Access other than read-only shall only be allowed after proper approval from the Lead - ISRC.
- Where system audits require access to production system or data or includes the use of software tools and utilities, such audits shall be conducted with the knowledge, cooperation and consent of the owners of the Information Systems.
- Relevant precautions shall be taken to protect the Information Systems and data from damage or disruptions as a result of the audit.

14. Communications Security Policy

14.1 Network Security Management (A.13.1)

Network Control (A.13.1.1)

- The responsibility of managing network devices shall be separated from those managing computer operations.
- Any change in the network environment shall be controlled, and authorized, and follow a documented change control procedure.
- Vulnerability assessment and penetration testing of all servers and networking devices shall be carried bi-annually and weaknesses identified shall be analysed and resolved.
- Access to Syngene network services shall be authorized, given on need to use basis and shall follow formal access control procedures.
- Connection capability of users to Syngene shared network shall be restricted through network gateways that filter traffic by means of pre-defined tables or rules in order to permit only authorized users.
- Appropriate routing controls shall be used to ensure that access to Syngene shared network is as per the defined access control policy

Security of Network Services (A.13.1.2)

- Network services (such as Email, FTP or Internet) which are allowed to be accessed and the security features required to maintain the integrity and availability of the network services shall be identified and documented.
- The ability of the network service provider to manage agreed services in a secure way shall be determined and regularly monitored, and the right to audit shall be agreed.
- Use of network services shall be monitored on a regular basis.
- Use of wireless networks shall not be permitted unless authorized for valid business purposes only.
- Secure authentication mechanisms shall be used for remote / external connections to the Syngene network.
- Any remote access to the Syngene network by a Syngene employee or a supplier shall be authorized.
- All activities performed through remote connectivity shall be logged and closely monitored.
- Connection capability of users to Syngene shared network shall be restricted through network gateways that filter traffic by means of pre-defined tables or rules in order to permit only authorized users.
- Where it is important that communication can be initiated only from a specific location or equipment, unique equipment identifiers shall be used to authenticate connections in addition to user authentication.
- Physical security of all such equipment shall be ensured to maintain the security of the equipment identifier.

- Appropriate routing controls shall be used to ensure that access to Syngene shared network is as per the defined access control policy.
- Access to all diagnostic and configuration ports on any Syngene information processing system shall be restricted to authorized personnel only.
- Any access to diagnostic and configuration ports, authorized to third party users, shall be monitored and all such access shall be limited only for the period of diagnostics.
- Ports or services installed on a computer or network facility, that are not required for business use shall be disabled.

Segregation in Networks (A.13.1.3)

- Syngene user network shall be segregated from the server network.
- Syngene internal network shall be segregated and adequately protected from the risks of connecting to other un-trusted or public networks.
- Syngene application servers shall be segregated from the database servers.
- Networks belonging to different missions shall be separated.
- Access between segregated networks shall be controlled by the access control policy and shall be based on the sensitivity of information and information processing systems within each network.
- Where it is important that communication can be initiated only from a specific location or equipment, unique equipment identifiers shall be used to authenticate connections in addition to user authentication.
- Physical security of all such equipment shall be ensured to maintain the security of the equipment identifier.

14.2 Information Transfer (A.13.2)

Information transfer policies and procedures (A.13.2.1)

Information transfer procedures and controls shall be established to protect the transfer of information through the use of all types of communication facilities. Following activities shall be adhered to:

- Exchange of information using various methods and formats (such as email, letter, fax etc.) shall be governed as per the Syngene's Asset Management Procedure
- Malwares/ virus that may be transferred through the use of electronic communications shall be detected and protected in accordance to Virus & Malicious Protection procedures.
- Information and data shall be protected with appropriate controls based on the information classification categories as per the Data Classification Policy
- Automatic forwarding of electronic mail to external addresses shall be restricted. Syngene personnel shall take appropriate precautions, not to reveal 'Confidential'

information and to avoid being overheard or intercepted when making a phone call by people in their immediate vicinity, wiretapping or people at the recipient end.

- Employees shall be periodically made aware about the security issues when any confidential information lying unsecured; and the importance of security of information when communicating.

Agreements on Information Transfer (A.13.2.2)

- Appropriate arrangements (Legal Agreements, Non-Disclosure Agreements etc.) shall be made for relationship with suppliers, clients or contractors as per the Supplier Relationship procedure to secure transfer of critical business information.
- For critical information transferred to suppliers, the information transfer agreement shall address the following criteria at a minimum:
 - Management Responsibilities;
 - Procedures to establish traceability and chain of custody;
 - Monitoring Requirements;
 - Reporting Security Incidents

Electronic Messaging (A.13.2.3)

- The organisation shall apply adequate controls on the mail servers to ensure correct addressing and transporting of messages.
- Mechanisms shall be defined to ensure appropriate approvals are obtained prior to allowing users to access external third-party mail or external file sharing services.
- Stronger cryptographic and security controls shall be implemented for publicly accessible resources like mailboxes or file servers.
- An email disclaimer shall be appended to any email sent out from Syngene. The IT Team shall be responsible to ensure that the latest disclaimer is being used while sending emails

Confidentiality and Non-Disclosure agreements (A.13.2.4)

- Critical business information shall be protected based on the Data Classification Policy. The agreements with the third parties shall address the following (not exhaustive):
 - Duration of agreement;
 - Permitted users of the information;
 - Required actions when agreement is terminated;
 - Right to monitor or audit clauses;
 - Need for compliance with applicable laws and regulations; and
 - Process for notification of breaches along with legal remedies.
- Based on the Syngene information security requirements and the sensitivity of the information involved, other clauses may be included. The clauses shall be periodically reviewed by the Legal team and updated to include latest changes in legal and regulatory requirements.

15. System Acquisition, Development and Maintenance Policy

15.1 Security Requirements of Information Systems (A.14.1)

Information Security Requirements Analysis and Specification (A.14.1)

- Security requirements shall be explicitly identified and documented as part of the requirements and design phase for all new Syngene business applications and enhancements to existing business applications.
- Information Security requirement shall take into consideration the following
 - The level of confidence required towards the claimed identity of the user
 - Access provisioning and authorisation processes.
 - User duties and responsibilities
 - Business requirements such as transaction logging and monitoring, non-repudiation etc.
 - Requirement mandated by other security controls
- For products that have been acquired, a formal testing and acquisition process shall be followed.
- Criteria for accepting the product shall be identified.

15.2 Security in Development and Support Processes (A.14.2)

Security in development process (A.14.2)

- All changes to existing business applications shall follow a defined change management process.
- All modifications to software packages shall be discouraged and only necessary changes shall be implemented
- IT shall establish secure development environments for specific system development efforts including people, processes, and technology associated with system development and integration
- Acceptance criteria for new Information Systems, upgrades / patches, and new versions shall be established and suitable tests of the system(s) shall be carried out prior to acceptance

15.3 Test Data (A.14.3)

Protection of Test Data (A.14.3)

- Any personal or confidential information on the operational system shall not be used as test data. If such information is used, it shall be sanitized before use.
- Access control procedures, which apply to operational application systems, shall also apply to test application systems.
- Operational information shall be erased from a test application system immediately after the testing is complete.

16. Supplier Relationship Policy

16.1 Information Security in Supplier Relationships (A.15.1)

Information Security Policy for Supplier Relationships (A.15.1.1)

- Syngene shall identify and mandate information security controls to specifically address supplier access to Syngene's information.
- These controls shall address the following:
 - identify and document the types of suppliers, e.g. IT services, logistics utilities, financial services, IT infrastructure components, whom the organization will allow to access its information;
 - a standardized process and lifecycle for managing supplier relationships;
 - minimum information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the Syngene's business needs and requirements and its risk profile;
 - handle incidents and contingencies associated with supplier access including responsibilities of both the Syngene's and suppliers;
 - conditions under which information security requirements and controls shall be documented in an agreement signed by both parties;
- Manage the necessary transitions of information, information processing facilities and anything else that needs to be moved and ensure that information security is maintained throughout the transition period.
- Formal procedures shall be established to ensure that security controls, service definitions and delivery levels included in the agreements with the suppliers are implemented, operated, and maintained by them
- All supplier access rights, logical as well as physical, shall be removed on termination of the supplier service.

Addressing Security with Supplier Agreements (A.15.1.2)

- Agreements with suppliers shall cover all relevant security requirements, including the right to audit, to ensure compliance with Syngene's security policies and procedures.
- Supplier agreements shall include each party's responsibilities, service definitions, service levels, change management procedure to be followed, escalation procedures and termination procedures.
- It shall be the responsibility of each supplier personnel to adhere to Syngene's policies and procedures applicable when handling and disposing Syngene's information or information processing systems and/or facilities
- Formal procedures, as defined in the supplier agreement, shall be followed for termination of a supplier engagement.

Information and Communication Technology Supply Chain (A.15.1.3)

- Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain
- Define information security requirements to apply to information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships
- Implement a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements
- Obtain assurance that critical components and their origin can be traced throughout the supply chain

16.2 Supplier Service Delivery Management (A.15.2)**Monitoring and Review of Supplier Services (A.15.2.1)**

- Control and visibility shall be maintained in all security aspects for sensitive or critical information or information processing systems and facilities accessed, processed or managed by an external party.
- Service performance reports produced by the third party shall be reviewed and regular progress meetings shall be arranged.
- In case of outsourcing arrangements, the supplier shall be audited periodically and all non-compliances to contractual requirements, operational issues, incidents and failures identified as part of the audits shall be reported.
- Suppliers shall plan and implement corrective and preventive actions for all audit findings.

Managing Changes to Supplier Services (A.15.2.2)

- Changes to the provision of services shall be managed taking into account the criticality of the business systems and processes involved, service delivery levels and re-assessment of risks.
- Changes to the provision of services shall follow the agreed upon change management procedure as defined in the agreement with the vendor.

17. Information Security Incident Management Policy

17.1 Management of Information Security Incidents and Improvements (A.16.1)

Responsibilities and Procedures (A.16.1.1)

- Syngene shall establish procedures to identify, record, categorize, prioritize and initiate resolution of various types of incidents.
- A root cause analysis for all P1 incidents shall be carried out to identify the underlying cause and prevent recurrence.
- Incident root cause analysis and classification shall be carried out by trained personnel and assigned to specific teams for incident resolution.
- The status of logged incidents shall be tracked and recorded.
- Incident Management process shall be guided by the service level agreements.
- Non-conformance to the agreed service levels shall be analysed and reasons shall be reported.
- The security incidents that cannot be resolved immediately shall be escalated and, if required, workarounds shall be provided.
- Any resolution that requires changes shall follow the Syngene's change management policy.
- Syngene shall ensure that all resolutions are accepted by the reporting users before the incidents are closed.
- All high impact incidents for which root cause could not be determined shall be escalated as a problem.

Reporting Information Security Events (A.16.1.2)

- Syngene shall train its employees, service providers and suppliers to identify different types of incidents and report them.
- Syngene reserves the right to monitor computer systems, network traffic and account and data usage, to assist in the detection, identification and management of security incidents and breaches
- Automatic monitoring of systems, alerts, and vulnerabilities shall be used to detect information security events in addition to reporting of incidents.
- Situations to be considered for information security event reporting include:
 - ineffective security control;
 - breach of information integrity, confidentiality or availability expectations;
 - human errors;
 - non-compliances with policies or guidelines;
 - breaches of physical security arrangements;
 - uncontrolled system changes;
 - malfunctions of software or hardware;
 - Access violations.
 - Fake / Fraudulent Websites

Reporting Information Security Weaknesses (A.16.1.3)

- Syngene users shall also report any security weaknesses related to systems and services to the Information Security Manager in order to prevent such weakness converting into an Information Security incident.
- Types of Information Security weaknesses that may include, but are not limited to the following:
 - Unauthorized disclosure of information;
 - Falsification of information;
 - Malicious code and hacker intrusion;
 - Unavailability of critical information asset; and
 - Installation of equipment not authorized by Syngene.
- Syngene shall provide ongoing awareness to the users on identifying an Information Security event and reporting such events to the appropriate parties.

Assessment of and Decision on Information Security Events (A.16.1.4)

- Upon receiving an information security event incident from the user, Syngene shall assess whether the event shall be classified as an information security incident and shall follow the “Syngene Incident Management Procedure” to further classify the information security incidents.

Response to Information Security Incidents (A.16.1.5)

- Syngene shall organize information security incident response team (ISIRT) to quickly respond to incident.
- All major incidents shall be communicated to senior management and relevant stakeholders and resolved on priority.
- All incidents shall have a responsible subject matter expert at all times.
- The response shall include:
 - Collecting evidence as soon as possible after occurrence;
 - Conducting information security forensic analysis;
 - Keep records of all response activities for future reference.
 - Incident records shall be periodically reviewed to ensure timely resolution of incidents.
- Syngene reserves the right to monitor computer systems, network traffic and account and data usage, to assist in the detection, identification and management of security incidents and breaches.

Learning from Information Security Incidents (A.16.1.6)

- The resolution of previously occurred incidents shall be made available to incident management team to make use of known errors and workarounds in restoring normal service to the business.
- Preventive measures shall be identified to avoid such occurrences in future.

Collection of Evidences (A.16.1.7)

- In the event of a security incident originated by employee or sub-contractors, the associated evidences shall be collected and preserved, irrespective of whether a legal action is required or not.
- Whenever applicable, evidence shall be collected by an authorized personal or a third-party nominated by the management and proper chain of custody shall be maintained.

18. Business Continuity Management Policy

18.1 Planning Information Security Continuity (A.17.1.1)

- The organization-wide Business Continuity Management processes shall include information security requirements to help ensure that confidentiality, integrity and availability of critical information assets shall be preserved even in the event of a business disruption or disaster.
- Syngene shall identify and document information system availability, resilience and recovery requirements in-line with the organization-wide Business Continuity Management requirements.
- Syngene shall define, document and implement Disaster Recovery plan in-line with the organization-wide Business Continuity Management requirements.
- Syngene shall identify and document business process interdependencies and relationships with other processes, services and underlying Information Systems.
- Syngene shall identify and document events that can cause possible interruptions to business processes along with the probability and impact of such interruptions and their consequences for business operations.
- Based on the identified impact of such interruptions and their consequences for business operations, Syngene shall identify acceptable service outage limits and data losses.
- Syngene shall define and document recovery guidelines that can be taken as baseline reference to classify mission critical systems and develop recovery and restoration procedures.

18.2 Implementing Information Security Continuity (A.17.1.2)

- A suitable Business Continuity Management framework that comprise of business continuity organization structure, roles and responsibilities, policies, procedures and measurement matrices shall be developed and implemented across the organization.
- The adopted Business Continuity Management framework shall cover the following:
 - the analysis of business process interdependencies and relationships;
 - the business impact analysis due to people, process, or technology outages and/or unavailability;
 - identification of threats to Business Continuity, likelihood of such threat and the corresponding risks exposure;
 - identification and selection of Business Continuity and Disaster Recovery strategies based on the identified acceptable service outage limits and data loses as well as the interdependencies and relationships between processes, services and underlying information systems;
 - development of Business Continuity and Disaster Recovery plans;

- development of Business Continuity test plans and test procedures;
- execution of Business Continuity and Disaster Recovery tests; and
- Updating and maintaining Business Continuity and Disaster Recovery plans.
- The adopted Business Continuity Management framework shall be aligned with Syngene goals and objectives and leading industry best practices.
- There shall be relevant business continuity plans, developed, implemented and maintained in order to continue or restore operations and ensure availability of the required information at the required time. Such procedures, systems and solutions implemented shall ensure that confidentiality and integrity requirements of Syngene critical information are also preserved at all times.

18.3 Verify, Review and Evaluate Information Security Continuity (A.17.1.3)

- Business Continuity plans shall be tested and updated regularly to ensure that they are up-to-date and effective.
- Disaster Recovery solutions and plans shall be tested regularly to ensure continued effectiveness of such arrangements.
- The Business Continuity and Disaster Recovery plans shall be tested based on a pre-determined schedule.
- The designated business process owners and team members shall be engaged in performing the Business Continuity and Disaster Recovery tests.
- The records and results of Business Continuity and Disaster Recovery testing shall be maintained.
- The results of Business Continuity and Disaster Recovery testing shall be used to enhance the Business Continuity and Disaster Recovery plans.

18.4 Availability of Information Processing Facilities (A.17.2.1)

- Syngene shall prepare and communicate the strategies for the redundancy requirements for information processing facilities to meet the availability requirements.
- Syngene shall implement the redundant information processing components and perform the tests as per the Recovery strategies defined within Business Continuity Plan.

19. Information Security Compliance Policy

19.1 Compliance with Legal and Contractual Requirements (A.18.1)

Identification of Applicable Legislation and Contractual Requirements (A.18.1.1)

- All relevant regulatory requirements shall be identified including the local statutory, regulatory and contractual requirements.

Intellectual Property Rights (IPR) (A.18.1.2)

- No employee or sub-contractors shall reproduce any intellectual work in violation to its copyright. This applies to any intellectual work protected by copyright law even if it was not produced in India.
- Information stored on Syngene system and network shall remain the property of Syngene and all employees and sub-contractors are bound by the Information Security policy.
- All intellectual property materials in use within Syngene shall be identified and documented.
- Inventory of proprietary software and relevant licenses used in Syngene shall be maintained.
- Appropriate procedures shall be implemented to ensure compliance with legal restrictions on the use of material with respect of intellectual property rights, and on the use of proprietary software products.

Protection of Records (A.18.1.3)

- Appropriate technical and procedural controls shall be implemented to protect Syngene' organizational records. These shall include but will not be limited to, records of business transactions, transaction logs, system audit logs, configuration settings, change control logs, user access logs, and authorization records.
- All such records shall be securely maintained, in electronic or hard-copy format, as required by legal, regulatory and industry specific requirements.
- Records shall be protected from loss, destruction, and falsification in accordance with business requirements and the requirements of the applicable laws and regulations of the country of operation.

Privacy and Protection of Personally Identifiable Information (A.18.1.4)

- All data protection and privacy requirements applicable across the locations of Syngene operations shall be identified and documented.
- Syngene shall implement adequate protection controls to ensure that an individual/employee's personal information is protected from misuse.
- Personal identifiable information shall only be collected and used for business purposes and in line with relevant legislations, regulations and contractual clauses.
- Personal information shall not be shared without due consent of the concerned individual or the approval of the HR department, except where Syngene may be

obligated to share such information with law-enforcement, government and regulatory authorities, or to prevent imminent loss or harm to the concerned individual or others.

- Communications that may include personal or private information such as email, phone calls and faxes made through Syngene systems and networks shall only be recorded and monitored in accordance with defined instructions, approvals and after informing the concerned individuals.

19.2 Information Security Reviews (A.18.2)

Independent Review of Information Security (A.18.2.1)

- Independent audits of operational information systems shall be performed as per the planned intervals or when significant changes occur.
- Audits shall be limited to read-only access to data. Access other than read-only shall only be allowed after proper approval from Information Security Committee.
- Relevant precautions shall be taken to protect the Information Systems and data from damage or disruptions as a result of the audit.
- Audit scope, procedures, responsibilities and resources involved shall be identified and documented.
- Syngene shall protect the integrity of audit results by applying appropriate access restrictions to information processing system audit tools.

Compliance with Security Policies and Standards (A.18.2.2)

- Continued compliance with Syngene Information Security policies and procedures shall be maintained.
- Any detected non-compliances with the Information Security policies shall be investigated and preventive action shall be taken and reviewed.
- Such non-compliances as well as their preventive actions shall be further reported at the time of independent reviews.

Technical Compliance Review (A.18.2.3)

- Compliance of Syngene Information Systems with technical security standards shall be maintained. Security control measures shall be regularly reviewed to ensure continued compliance with ISMS.
- In case of any non-compliance, a root-cause analysis shall be performed to ascertain the reasons and possible preventive actions for the future.
- Wherever any access to production data is required for audit purposes, access shall be given as read only and all such access to the data shall be revoked immediately after the audit work is over.

20. Mobile Device Management Policy

The purpose of this document is to ensure that anyone who is using a mobile computing device (including smartphone, tablet, laptop, etc.) to process or store Syngene data is aware of and agrees to adhere to this policy

Mobile Device Security

- Mobile Device Management (MDM) System shall be implemented in the enterprise network to enhance the security of corporate information on individual's devices. The features of MDM shall include the following:
 - Unauthorized apps shall be prevented from accessing the email data
 - Selective wipe out of corporate email account shall be facilitated if employees lose their devices
 - MDM shall restrict users to download attachments, forwarding to external domains to ensure security of data
- Employees having access to corporate email on their personal devices, are required to enforce to two factor authentication.
- MDM procedures which state the process of enrolling employees in MDM shall be defined and communicated
- Employees shall enrol themselves for mobile management by adding their work account to their devices
- Employees need to accept and install a mobile device management policy and a synchronization process to connect to Syngene's domain
- Mobile emails shall be secure by enabling appropriate encryption and decryption
- System / Network administrator shall:
 - View device activity from the Admin console or Admin app
 - Use audit logs to see individual event details
 - Detect activity that indicates policy non-compliance
 - Block or remove an account from the device

21. Acceptable Usage Policy

Syngene users shall be required to read and formally sign the Acceptable Usage Policy before gaining access to Syngene information system and/or services.

General Employee Responsibilities

- All users shall take necessary steps to prevent unauthorised access to confidential information.
- Users shall not attempt to circumvent Syngene's security measures or attempt to gain unauthorised access to secured or protected files on a computer system.
- All users shall be responsible for the security of the equipment allocated or used by them and must not allow it to be used by anyone else.
- All users shall be responsible for protecting their passwords from unauthorised disclosure and for changing passwords regularly
- Employees are responsible for protecting their own encryption passwords, passphrases, PIN codes and a secure backup of any keys provided
- Managing private encryption keys is the responsibility of the individual. The keys and passphrases must never be shared or given out to anyone
- Syngene IT Resources must not be used for personal benefit, political activity, unsolicited advertising, unauthorised fund raising, or for the solicitation of performance of any activity that is prohibited by any law

Information Systems and Services Usage

- All users shall take due care to protect Syngene's Information Systems and resources from unauthorized access, tampering and/ or accidental damage.
- All Syngene's Information Systems including desktops, laptops, mobile devices, printers, fax machines, photocopiers, as well as servers and applications shall only be used for their intended and authorized business purposes.
- Users shall not use Syngene provided facilities and services for illegal or unlawful purposes, including but not limited to copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses).
- Users shall not use Syngene's systems or networks to access unauthorized systems, networks and/or services.
- Users shall not install any software or applications which is not included within the authorized software list into desktops or laptops given by Syngene for business purposes.
- Users with administrative rights shall not disable or by-pass any controls such as anti-virus software, proxy servers and/or firewalls implemented to protect Syngene information assets. Such by-pass shall be considered as an Information Security

violation and may lead to disciplinary actions according to Syngene Disciplinary policy.

- Users with administrative rights shall not install unacceptable software including but not limited to Peer-to-Peer (P2P) software, Network Scanning or Hacking tools on their devices unless authorized by Syngene.
- Users with administrative rights shall not install any software that does a similar function to a standard Syngene software like internet browsers, anti-virus or anti-spyware software.
- Users with administrative rights shall not install any pirated software.
- Each user of Syngene shall be allocated a limited server usage space for storing their business-related data. The data/ information contained within such user folders shall be under the custody of the respective users. Users shall not store unauthorized content in such folders.
- Users shall be strongly encouraged to save their critical data to the appropriate servers so that these data can be backed up regularly.

Information Usage

- Users shall not disclose, communicate or discuss in public any of Syngene's confidential or highly confidential information.
- Users shall not post any Syngene related confidential / highly confidential information on publicly accessible internet sites such as mailing lists or public news groups without obtaining appropriate approval.
- Users shall obtain appropriate intellectual property rights / copyright or contractual clearances before using any proprietary material. Using or providing Syngene developed software, innovative ideas, designs or repositories (software or otherwise) outside Syngene environment is prohibited.
- Users shall use, handle and treat all information in accordance with the Asset Management procedure.
- Users shall not transmit confidential / highly confidential information over the network without adequate protection controls.
- Before sharing any information about the Syngene environment, users shall confirm the identity and the "need-to-know" of the recipient.

Email Usage

- Email access at Syngene shall be controlled through individual account and password. It shall be the responsibility of the employee to protect the confidentiality of their account and password information.
- E-mail accounts shall be granted to sub-contractors on a case-by-case basis with appropriate approval by departmental heads.
- Email users shall be responsible for the management of the mail space allotted, including the responsibility of deleting old & junk mails.

- Users shall use the organization's standard e-mail signature templates in all e-mail communications.
- Email access shall be terminated when the employee or third party terminates their association with Syngene. Syngene is under no obligation to store or forward the contents of an individual's email inbox/outbox after the term of their employment has ceased.
- Sending unsolicited marketing or commercial email (i.e. 'spam') is strictly prohibited. 'Spamming' could result in a substantial liability to Syngene or cause significant reputation harm to its brands
- Email marketing must only be carried out by our Marketing function in accordance with established business practices and our Marketing Policies
- Always double-check that the recipients are correct BEFORE hitting SEND for Confidential or Highly Confidential information in an email
- Auto-forwarding of email to external email addresses is prohibited as it can lead to Syngene sensitive information being sent over the internet in an unprotected fashion
- Employees should exercise particular caution when opening unsolicited e-mails from unknown sources, an e-mail which appears suspicious (for example, if it contains a file whose name ends in .exe) or clicking on a link by considering whether the link makes sense from a business perspective and whether it comes from a source you know and trust. Targeted email (Phishing) attempts should be reported to IT department immediately.
- Personal email services (e.g. Gmail) must not be used for conducting Syngene business
- Employees must only send email from email addresses they are authorised to use
- Employees must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory or otherwise inappropriate e-mails
- Anyone who feels they have been harassed or bullied or are offended by material received from a colleague should inform their line manager/HR
- Employees must take care with the content of e-mail messages as incorrect or improper statements can put the company at risk of claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract
- Always assume that e-mail messages will be read by others and do not include anything which would offend or embarrass the company, reader, or yourself, if it found its way into the public domain
- Never agree to terms, enter into contractual commitments or make legal representations by e-mail unless authorised to do so.
- Never download or e-mail text, music and other content on the internet which is copyright protected unless it is clear that the owner of the material allows this.
- Employees should return misdirected e-mail to the sender.
- Double-check your content does not contain inappropriate Confidential or Highly Confidential Information when forwarding email to outside parties

- Confidential or Restricted content must only be emailed to non-Syngene staff with valid business reason in accordance with the Data Classification Policy.
- Always encrypt Confidential or Restricted attachments when sending email outside of Syngene in accordance with the Data Classification Policy.
- Employees must retain and dispose of emails in accordance with the Asset Management procedure.
- Care must be taken in using digital signatures in email because of the opportunities for forgery

Internet Usage

- Users shall use Syngene Internet services appropriately, responsibly and ethically.
- The Internet access may not be used in a way that violates Syngene policies, rules or administrative orders.
- Users shall only use Syngene Internet services for business related activities. The illegal or non-business use of such services is not permitted.
- Users shall not use Syngene Internet services for illegal or unlawful purposes, including but not limited to copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses). Any such activity may result in disciplinary action in-line with the Syngene Disciplinary Policy.
- Users shall be solely responsible for the content they disseminate or information they access through the internet services provided by Syngene.

Instant Messaging Usage

- Syngene approved tools (Microsoft Teams) are to be used for internal communications (incl. trusted third parties).
- Users must not be used to record information that users are expected to retain as evidence of a business transaction
- Users must never share commercial information (e.g. pricing, discounts, margins, etc.), or any other confidential or highly confidential information
- Users shall not formalize or enter into contracts, agreements or commitments.
- Users shall never share images or content that may be considered embarrassing, explicit, profane, sexually obscene, threatening, harassing, discriminatory or offensive.
- Users shall never share information with third parties you do not know.
- While sharing desktops and exchanging documents, care must be exercised when communicating and/or receiving files from external parties.
- Users shall not leave the desktop share unattended. If an individual gives control of his/her desktop to you, disconnect immediately when the session is over.
- Email Usage guidance (as above) also applies when using Instant Messaging.

Password Usage

- Passwords shall be the first line of defence for protecting assets and the acceptable use of passwords.

Printer & Fax Usage

- Collect the printed copies as soon as it is printed. If the printed copy is no longer required, dispose it appropriately.
- Confidential documents shall not be printed on publicly accessible printers without the direct supervision and presence of an authorized person.
- Make efforts to limit paper usage by taking advantage of duplex printing and other optimization features.
- The recipient shall be notified prior to the transmission.
- Obtain and file a 'fax received' confirmation receipt.

Remote Access

- It is the responsibility of any Syngene user with remote access privileges to ensure that their remote access connection remains as secure as possible.
- Any remote connection that is configured to access Syngene resources shall adhere to Syngene Information Security policies, procedure and standards.
- Do not leave sessions unattended and always log out from the session when finished

Monitoring

- Syngene may monitor aspects of its computer systems, including internet activity (e.g. as part of an investigation or incident) to protect Syngene and maintain compliance to Syngene policies as permitted by local law. This may include, but is not limited to:
 - chat rooms, newsgroups, social networking and instant messaging material, downloads and uploads of information by employees
 - email sent or received
 - files shared on cloud file sharing sites
- Syngene reserves the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interest of the business, including the following purposes (but not limited to):
- to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with Syngene policies
 - to find lost messages or to retrieve messages lost due to computer failure
 - to assist in the investigation of alleged wrongdoing
 - to comply with any legal obligation

22. Exceptions

In the event that a valid business reason exists for controls within an environment to be exempted from complying with Syngene' s Information Security policy, then the following procedure shall be followed: -

- A descriptive reason shall be submitted to the Lead – ISRC.
- The Lead - ISRC shall evaluate the risk and compile a report. The report shall be submitted to the ISC to seek formal approval for the exclusion

23. Revision History:

Version Number	Summary of Changes	Effective Date	Remarks
001	Newly Introduced	01.02.2019	
002	Annual Review with no changes	02.01.2020	
003	Annual Review with no changes	04.01.2021	