

Synrgise Learn Information Security Policy

Document Control

Version: v1.2

Date: 2023

Distribution: All

1	Synrgise Learn ISMS Policy	7
2	Introduction.....	10
2.1	Need for a Security Policy	10
2.2	Legal Requirements	10
2.3	Purpose and Scope of the Policy	10
2.4	Who is affected by the Policy	11
2.5	Where the Policy Applies	11
2.6	Security Policy Objectives.....	11
2.7	Review and Audit	11
3	Acceptable Use	12
4	Security Management and Responsibilities	13
4.1	Objective	13
4.2	Synrgise Learn's Responsibility	13
4.3	Head of Information Compliance & Policy	13
4.4	Data Owner	13
4.5	Systems Development	14
4.6	Change Management	14
4.7	Management Responsibilities	14
4.8	Employees Responsibilities	14
4.8	System Managers	14
5	Enabling the flow of information	16
5.1	Objective	16
5.2	Sharing data/information with other organisations.....	16
5.3	Sharing data/information with non-partner organisations	16
5.4	Objective	16
5.5	Network Security	17
5.6	Telephone Security	17
5.7	Email (see also specific Email section)	17
5.8	Internet	17
5.9	Verbal Communications	17
6	Risk Management	17
6.1	Objective	17
6.2	Risk assessment	17
6.3	Threats	18

6.4	Vulnerabilities	18
6.5	Risk Register	18
6.6	Risk Treatment	18
6.7	Roles and Responsibilities	19
6.8	Risk Appetite and Tolerance	19
7	Awareness.....	19
8	Confidentiality Agreements.....	20
9	Business Continuity.....	21
9.1	Objective	21
9.2	Need for effective plans	21
9.3	Planning process	21
9.4	Planning framework	21
10	Equipment and Software Registers	23
10.1	Objectives	23
10.2	Equipment Inventory	23
10.3	Software Register	23
11	Access control to secure areas	24
11.1	Objective	24
11.2	Physical security	24
11.3	Entry controls	24
12	Security of Third Party Access	25
12.1	Objective	25
12.2	Access control	25
13	User Access Control.....	26
13.1	Objective	26
13.2	Access to Systems.....	26
13.3	Eligibility	26
13.4	Registering users.....	26
13.5	User password management.....	26
13.6	Employees leaving Synrgise Learn's employment.....	27
13.7	Visitors and Contractors	28
13.8	The Internet	28
14	Housekeeping.....	29
14.1	Objective	29
14.2	Data Backup.....	29
14.3	Equipment, Media and Data Disposal	29

15	Software and Information Protection	30
15.1	Objective	30
15.2	Licensed software	30
15.3	Unauthorised Software	30
15.4	Virus control	30
15.5	Time-out procedures	31
16	Equipment Security	31
16.1	Objective	31
16.2	Equipment sitting and protection	31
16.3	Power supplies	31
16.4	Network Security	31
16.5	Use of '3G modems' and other communications equipment	32
16.6	Portable & Hand-held Computing Equipment	32
16.7	System Documentation	32
17	Incident Management	33
17.1	Incident Communication	33
17.2	Incident Registration	34
17.3	Incident Evaluation	34
17.4	Incident Notification	35
18	Electronic Mail (Email) Policy	39
18.1	Policy	39
18.2	Care in drafting Emails	39
18.3	Viruses and Attachments	39
18.4	Information Confidentiality	39
18.5	Intent to enforce and monitor	39
18.6	Retention and Purging	39
18.7	Junk mail	39
18.8	Very large files	40
18.9	Protection of your terminal	40
18.10	Mail Storms	40
19	Client and Corporate Record Storage & Transportation	41
19.1	Objective	41
19.2	Storage	41
19.3	Offices	41
19.4	Elsewhere	41

19.5	Transportation	41
19.6	Responsibility	41
20	Home working Information Security Standards.....	42
20.1	Objective	42
20.2	Authorisation to remove data files	42
20.3	Transfer of personal data files	42
20.4	Protecting data files	42
20.5	Use of Privately owned Computers at Home	42
20.6	Transportation of data or confidential documents.....	42
20.7	Storage of equipment	42
20.8	Storage of confidential data or reports	43
21	Appendix A: The Policy Review Process	44
21.1	Periodic reviews of policy documents	44
21.2	What the policy review should include.....	44
21.3	The review committee	44
22	Appendix B: Antivirus Guidelines.....	45
22.1	What is a Virus?	45
22.2	What does Synrgise Learn do to prevent the spread of viruses?	45
22.3	Avoid Unauthorised Software	45
22.4	Treat All Attachments with Caution	45
22.5	Avoid Unnecessary Macros	46
22.6	Be Cautious With Encrypted Files	46
22.7	Suspicious Filename Extensions	47
23	Appendix C: Risk Assessment Template	48
23.1	Guidance on usage	48
23.2	Guidance on scoring	49
24	Appendix D: IT Change Management Policies and Procedures.....	50
24.1	Introduction	50
24.2	Scope	50
24.3	Purpose	50
24.4	References and definitions	51
24.5	Normative references	51
24.6	Definitions and abbreviations	51
24.7	Policy	52
24.8	Preamble	52

24.9	Roles and Responsibilities	56
24.10	Compliance	58
24.11	IT Governance Value statement	58
24.12	Policy Access Considerations	58
25	Glossary & Abbreviations	59
26	References	61

1 Synrgise Learn ISMS Policy

Purpose

The purpose of this policy is to protect from all threats, whether internal or external, deliberate or accidental, the information assets of:

Synrgise Learn;

Customers;

Suppliers;

Objectives

The implementation of this policy is important to maintain and demonstrate our integrity in our dealing with customers and suppliers.

It is the policy of Synrgise Learn to ensure:

- Information is protected against unauthorised access
- Confidentiality of information is maintained
- Information is not disclosed to unauthorized persons through deliberate or careless action
- Integrity of information through protection from unauthorised modification
- Availability of information to authorized users when needed
- Regulatory and legislative requirements will be met
- Business continuity plans are produced, maintained and tested as far as practicable
- Information security training is given to all Employees
- All breaches of information security and suspected weaknesses are reported and investigated

Applicability

All Synrgise Learn personnel and suppliers, employed under contract, who have any involvement with information assets covered by the scope of the Information Security Management System, are responsible for implementing this policy and shall have the support of the Synrgise Learn Management who have approved the policy.

Goals

To identify through appropriate risk assessment, the value of information assets, to understand their vulnerabilities and the threats that may expose them to risk.

To manage the risks to an acceptable level through the design, implementation and maintenance of a formal Information Security Management System.

To comply with legislation including;

- Companies Act
- Health and Safety Act
- Electronic Communication Act
- The Protection of Personal Information Act
- Copyright Act
- Promotion of Access to Information Act
- Human Rights Act

To comply with any customer contract conditions relating to information security.

Commitment to comply with ISO 27001-2005

Commitment to achieve certification to ISO27001-2005

Specific Policies

Specific policies exist to support this document including:

- Physical Security
- Site access control policy (key holders, wearing of badges, visitor controls)
- Computer usage policy (email, internet access, access control, software download)
- Password controls (frequency of change, length, complexity)
- Data backup
- Virus control policy (frequency of updates, control of external media)
- Communications policy
- Business Continuity Management
- Security breach and incident management policy

Responsibilities

The management of Synrgise Learn create and review this policy.

The Information Security Manager facilitates the implementation of this policy through the appropriate standards and procedures.

All personnel and contracted suppliers follow the procedures to maintain the information security policy.

All personnel have a responsibility for reporting security incidents and any identified weaknesses.

Any deliberate act to jeopardise the security of information that is the property of Synrgise Learn or their customer or suppliers will be subject to disciplinary and/or legal action as appropriate.

Review

The policy is reviewed bi-annually and in case of influencing changes to ensure it remains appropriate for the business and our ability to serve our customers.

Signed

Xenothan Hojem

Group CTO and ISMS Policy Owner

Date

2 Introduction

This Policy has been developed to protect all systems within Synrgise Learn to an adequate level from events which may jeopardize Organization activity. These events will include accidents as well as behaviour deliberately designed to cause difficulties.

2.1 Need for a Security Policy

The data stored in manual and electronic systems used by Synrgise Learn represent an extremely valuable asset. The increasing reliance on information technology for the delivery of Organization service makes it necessary to ensure that these systems are developed, operated, used and maintained in a safe and secure fashion in addition to paper based records.

The increasing need to transmit information across networks of computers renders the data more vulnerable to accidental or deliberate unauthorised modification or disclosure.

2.2 Legal Requirements

Some aspects of information security are governed by legislation, the most notable South African Acts are:

- Companies Act
- Health and Safety Act
- Electronic Communication Act
- The Protection of Personal Information Act
- Copyright Act
- Promotion of Access to Information Act
- Human Rights Act

2.3 Purpose and Scope of the Policy

The purpose of security in any information system, computer installation or network is to preserve an appropriate level of the following:-

Confidentiality the prevention of the unauthorized disclosure of information.

Integrity the prevention of the unauthorized amendment or deletion of information.

Availability the prevention of the unauthorized withholding of information or resources.

The level of security required in a particular system will depend upon the risks associated with the system, the data held on the system and the working environment of the system.

This policy applies to all information held in both manual and electronic form.

2.4 Who is affected by the Policy

The Policy applies to all employees of Synrgise Learn. It also applies to contractors and visitors, not employed by Synrgise Learn but engaged to work with or who have access to Synrgise Learn information, e.g. computer maintenance contractors.

2.5 Where the Policy Applies

The Policy applies to all locations from which Synrgise Learn systems are accessed (including home use). Where there are links to enable non-Synrgise Learn organizations (to have access to Synrgise Learn information, Synrgise Learn must confirm the security policies they operate meet our security requirements or the risk is understood and mitigated.

The Policy applies to all systems and all information whether commercial, administrative or any other.

2.6 Security Policy Objectives

- To ensure each member of Employees has a proper awareness and concern for computer systems security and an adequate appreciation of their responsibility for information security.
- To ensure all contractors and their employees have a proper awareness and concern for security of Synrgise Learn information.
- To provide a framework giving guidance for the establishment of standards, procedures and computer facilities for implementing computer systems security.
- To meet the general objectives of ISO27001 Code of Practice for Information Systems Security.
- To specify Synrgise Learn responsibilities.
- To ensure all Employees have an awareness of the Data Protection Act (1998) and its implications.
- To ensure that all Employees have an awareness of the Computer Misuse Act 1990.
- To ensure that all Employees are aware of their accountability and that they are aware that failure to comply with the Information Security Policy is a disciplinary offence which may include action up to and including summary dismissal. Any action taken will conform to the appropriate Synrgise Learn Human Resource policies.

2.7 Review and Audit

The Head of Information Compliance and Policy is responsible for regular review of the Policy in the light of changing circumstances. The review will occur annually or when there are significant changes. Synrgise Learn's Internal Audit Office has a brief to ensure that the Policy is appropriate for the protection of Synrgise Learn's interests.

3 Acceptable Use

All use of computer systems will comply with the Computing Services Acceptable Use Policy. Acceptable use is defined as use for the purposes of:

- Organizational business
- Research
- Personal educational development
- Administration and management of Organization business
- Development work and communication associated with the above
- Consultancy work contracted to Synrgise Learn
- Reasonable use of computer facilities for personal correspondence, where not connected with any commercial activity, is at present regarded as acceptable.

It is Synrgise Learn policy that all use of the facilities shall be lawful, honest and decent, and shall have regard to the rights and sensitivities of other people.

4 Security Management and Responsibilities

4.1 Objective

To ensure that Employees are aware of security risks and their responsibilities to minimise the threats.

Rationale – Information Security is a shared responsibility. Confidentiality, integrity and availability of information could be compromised due to a breach of security (which could be accidental or malicious) occurring at any point in the information flow.

4.2 Synrgise Learn's Responsibility

Synrgise Learn's policy is to accept all reasonable obligations in respect of information security and to protect its information resources by implementing best practices which achieve an effective balance between cost and risk.

4.3 Head of Information Compliance & Policy

The Head of Information Compliance & Policy is responsible for providing help and guidance on all matters relating to information security BUT ultimately data owners are responsible for ensuring compliance with the above policy statements and that the systems under their control have an appropriate level of security.

4.4 Data Owner

Each department with their own computer system will appoint a senior member of Employees as the Data Owner. Key responsibilities include:

- Data subject enquiry procedures
- To ensure, in liaison with Computing Services, the software licence to use the system is accurate, available and purchased according to financial regulations
- Preparing details of who can access what information, how and when, according to the particular classification of the information.
- Ensuring that the system is maintained in an effective and controlled manner.
- Ensuring that Employees immediately reports any violations or misuse of the system to them. The Data owner will then report it to Computing Services, if necessary.
- Application training and password control.
- Media and equipment disposal procedures in liaison with the COMPUTING SERVICES.
- Liaison with Head of Information Compliance & Policy.
- Those systems which are operated throughout Synrgise Learn should also have a designated Data Owner.
- The Head of Information Compliance & Policy will offer advice to data owners as to how they can manage their responsibilities. With existing systems, advice is available to help data owners meet their responsibility in complying with the Information Security Policy. With new and proposed systems, advice must be sought at the planning and development phase to ensure systems will meet the security policy requirements before purchase and installation.

4.5 Systems Development

All system developments must comply with the I.T. Strategy for Synrgise Learn. All system developments must include security issues in their consideration of new developments, seeking guidance from the Head of Information Compliance & Policy where appropriate.

4.6 Change Management

All system development, both internal and client solution based must comply with the change management procedure as outlined the Change Management Procedure (Appendix D).

4.7 Management Responsibilities

It is the responsibility of managers to ensure the following, with respect to their Employees: All current and future Employees should be instructed in their security responsibilities.

- Employees using computer systems/media must be trained in their use
- Employees must not be able to gain unauthorised access to any of Synrgise Learn IT systems or manual data which would compromise data integrity.
- Managers should determine which individuals are given authority to access specific information systems. The level of access to specific systems should be on a job function need, irrespective of status.
- Managers should implement procedures to minimise the organization's exposure to fraud, theft or disruption of its systems such as segregation of duties, dual control, peer review or Employees rotation in critical susceptible areas.
- Current documentation must be maintained for all critical job functions to ensure continuity in the event of relevant Employees being unavailable.
- All Employees should be aware of the confidentiality clauses in their contract of employment.
- Managers must ensure that the relevant system managers are advised immediately about Employees changes affecting computer access (e.g. job function changes leaving department or organisation) so that passwords may be withdrawn or deleted as appropriate.
- Managers must ensure that all contractors undertaking work for Synrgise Learn have signed confidentiality (non-disclosure) undertakings.
- Managers should ensure that all Employees have access to and have read Synrgise Learn Information Security Policy.

4.8 Employees Responsibilities

- Each employee is responsible for ensuring that no breaches of information security result from their actions.
- Each employee is responsible for reporting any breach, or suspected breach of security.

4.8 System Managers

- Job descriptions for system managers will include specific reference to the security role and responsibility of the post.

- The IT systems within Synrgise Learn should have a minimum of two, preferably three individuals with the expertise to manage or administer such a system.
- System Managers will be responsible to the Head of Information Compliance & Policy for continued system security.
- System Managers are responsible for promptly issuing user accounts.
- System Managers must ensure that only those persons who are authorised to have access are provided with that capability.

5 Enabling the flow of information

5.1 Objective

To enable the efficient flow of information without compromising its integrity and confidentiality.

5.2 Sharing data/information with other organisations

Synrgise Learn works with partner organisations which all have a legitimate role to play in delivering services and products. Partners, in this context, are taken to be, but not limited to:

- Suppliers
- Private sector providers
- Advertisers
- Consultants

A formal Information Sharing Protocol will, in time, be developed, which will make the standards of information protection control explicit, rather than implicit.

5.3 Sharing data/information with non-partner organisations

Synrgise Learn receives regular requests for personal data. Organisations requesting such information include:

- The Police
- Insurance companies
- Solicitors
- Potential employers

Whilst such requests may be legitimate, Synrgise Learn will ensure the use of such information is not abused and is in line with the Protection of Personal Information Act, by applying the following principles when considering the release of the information to non-partner organisations:

- Information will not be released without the consent of the individual concerned
- The Police will be asked to provide a legal documentation

These requirements may be waived in certain conditions (e.g. as a result of a court order, or where this information is required by law) but only after authorisation has been obtained from Synrgise Learn Secretary with will seek guidance if required from the Head of Information Compliance & Policy. Communications

5.4 Objective

To ensure that Synrgise Learn uses electronic, postal and verbal communications appropriately.

5.5 Network Security

Synrgise Learn will engage a third-party specialist to routinely review network security.

5.6 Telephone Security

Synrgise Learn management will ensure that Employees are aware of the importance of checking the credentials of all callers requesting personal or otherwise sensitive information.

5.7 Email (see also specific Email section)

Email should be used according to the conditions described here. The use of email may be monitored.

5.8 Internet

You should be aware of, and abide by the Computing Services Conditions of Use. Use of the Internet may be monitored. Please refer to the Internet Acceptable Use Policy.

5.9 Verbal Communications

Synrgise Learn management will ensure that all Employees are advised and regularly reminded of their obligation to respect the privacy of Employees. This means holding conversations discreetly and with due regard to the sensitivity of the subject under discussion.

6 Risk Management

6.1 Objective

To identify and counter possible threats to Synrgise Learn's information security and standards.

An assessment of all risks will be made for each information system to ensure that it is secured appropriately and cost effectively. Information systems within Synrgise Learn face many risks which a Security Policy can reduce or eradicate.

6.2 Risk assessment

Risk assessments must be completed with access to and an understanding of:

Synrgise Learn's business processes

- The impact to Synrgise Learn of risks to business assets
- The technical systems in place supporting the business
- The legislation to which Synrgise Learn is subject
- Up-to-date threat and vulnerability assessments

A risk assessment exercise must be completed at least:

- For every new information-processing system
- Following modification to systems or processes which could change the threats or vulnerabilities
- Following the introduction of a new information asset
- When there has been no review in the previous three years

A risk score is calculated from Likelihood x Impact Level, consistent with Synrgise Learn's Risk Management Policy (Appendix C).

6.3 Threats

Synrgise Learn will consider all potential threats applicable to a particular system, whether natural or human, accidental or malicious.

Synrgise Learn will reference Annex C of the ISO 27005 standard to aid with threat identification.

Threat information will be obtained from specialist security consultancies, local and national law enforcement agencies and security services, and contacts across the sector and region.

It is the responsibility of the Information Security Manager to maintain channels of communication with appropriate specialist organisations.

6.4 Vulnerabilities

Synrgise Learn will consider all potential vulnerabilities applicable to a particular system, whether intrinsic or extrinsic.

Synrgise Learn will reference Annex D of the ISO 27005 standard to aid with vulnerability identification.

Vulnerability information will be obtained from specialist security consultancies, local and national law enforcement agencies and security services, technology providers and contacts across the sector and region.

It is the responsibility of the Information Security Manager to maintain channels of communication with appropriate specialist organisations.

6.5 Risk Register

The calculations listed in the risk assessment process will form the basis of a risk register (Appendix C).

All risks will be assigned an owner and a review date.

The risk register is held in the Information Security document store, with access controlled by the Information Security Manager.

6.6 Risk Treatment

The risk register will include a risk treatment decision. The action will fall into at least one of the following categories:

- Tolerate the risk – where the risk is already below Synrgise Learn's risk appetite and further treatment is not proportionate
- Treat the risk – where the risk is above Synrgise Learn's risk appetite but treatment is proportionate; or where the treatment is so simple and cost effective that it is proportionate to treat the risk even though it falls below Synrgise Learn's risk appetite
- Transfer the risk – where the risk cannot be brought below Synrgise Learn's risk appetite with proportionate treatment but a cost-effective option is available to transfer the risk to a third party
- Terminate the risk – where the risk cannot be brought below Synrgise Learn's risk appetite with proportionate effort/resource and no cost-effective transfer is available

The Information Security Manager in collaboration with the Information Asset Owner will review Medium and Low risks and recommend suitable action.

The Information Security Board in collaboration with the Information Asset Owner will review High risks and recommend suitable action.

In the event that the decision is to Treat, then additional activities or controls will be implemented via a Risk Treatment Plan.

6.7 Roles and Responsibilities

The Chair of the Information Security Board has accountability to the Executive Group and Vice Chancellor for managing information risk.

They will direct the information risk appetite for Synrgise Learn and review the information risk register. They will be involved in assessing and reviewing High risks via the Information Security Board.

The Information Security Manager is responsible to the Chair of the Information Security Board for managing the risk assessment process and maintaining an up-to-date risk register. The Information Security Manager will conduct risk assessments and recommend action for Medium and Low risks, where these can be clearly defined in terms of Synrgise Learn's risk appetite.

The Information Security Board is responsible for assessing and reviewing High risks, and will have visibility of the risk register.

Information Asset Owners and Information Asset Managers must be responsible for agreeing and implementing appropriate treatments to risks under their control. They must also take an active role in identifying and reporting new risks.

6.8 Risk Appetite and Tolerance

Synrgise Learn has agreed a series of risk appetite statements.

While not exhaustive, these give a good overview of Synrgise Learn's desire to pursue or tolerate risk in pursuit of its business objectives.

The risk appetite statements give the Information Security Manager, and the Information Security Board, a framework within which to conduct risk assessments and make recommendations for appropriate treatments.

7 Awareness

Managers are responsible for ensuring that all Employees are aware of and adhere to this Information Security Policy. Computing Services will ensure that Security is included in all Computer User Training. Departmental managers are responsible for ensuring their Employees attend these awareness sessions.

Awareness material about Information Security will be made available as part of Synrgise Learn's intranet.

In order to maintain Synrgise Learn's information security and integrity, departmental managers must view Information Security training with the same gravity as Health and Safety training.

8 Confidentiality Agreements

Synrgise Learn will continue to adopt comprehensive policies and procedures to ensure the secure handling of personal information within all information environments such as complying with the Data Protection Act 1998.

Computer system users should sign an appropriate confidentiality (non-disclosure) undertaking. This should be part of the contract of employment for all Employees, however this applies particularly to Employees with access to sensitive data or systems. Before signing, each employee should have the conditions carefully explained by the Director or other such officer delegated by them.

Agency Employees and third party users not already covered by an existing contract (containing the confidentiality undertaking) should be required to sign a Confidentiality Agreement prior employment/registration. These Confidentiality Agreements should be reviewed when there are changes to terms of contract, particularly when systems are upgraded or contracts are due to end.

9 Business Continuity

Departmental management will be responsible for their department's contingency plan, its ongoing review and maintenance. This should be seen as part of the wider organisational plan.

Computing Services will be responsible for the technical aspects of all contingency plans and can provide advice on aspects of system data "catch up". They will maintain a Disaster Recovery Plan to ensure that all critical systems can be restored if necessary.

9.1 Objective

To be able to restore computer facilities to maintain essential business activities following a major failure or disaster.

9.2 Need for effective plans

Synrgise Learn recognises that some form of disaster may occur, despite precautions, and therefore seeks to contain the impact of such an event on its core business through tested disaster recovery plans.

Synrgise Learn recognises that IT systems are increasingly critical to its business and that the protracted loss of key systems/user areas could be highly damaging in operational terms.

Synrgise Learn requires tried and tested disaster recovery plans for its computing facilities to be maintained.

9.3 Planning process

The main elements of this process will include:-

- identification of critical computer systems
- identification and prioritisation of key users/user areas
- agreement with users to identify disaster scenarios and what levels of disaster recovery are required
- identification of areas of greatest vulnerability based on risk assessment
- mitigation of risks by developing resilience
- developing, documenting and testing disaster recovery plans identifying tasks, agreeing responsibilities and defining priorities

9.4 Planning framework

Disaster recovery plans will cater for different levels of incident including:-

- loss of a key user area within a building
- loss of a key building
- loss of a key operational area
- loss of a key part of a computer network
- loss of a computer's processing power
- loss of key Employees

Disaster recovery plans will always include:-

- emergency procedures covering immediate actions to be taken in response to an incident (e.g. alerting disaster recovery personnel)

- fallback procedures describing the actions to be taken to provide contingency devices defined in the disaster recovery plan
- resumption procedures describing the actions to be taken to return to full normal service
- testing procedures describing how the disaster recovery plan will be tested
- evidence of regular and adequate testing of Disaster Recovery Plans

10 Equipment and Software Registers

10.1 Objectives

To identify the location and authorised use of Synrgise Learn's computer assets

10.2 Equipment Inventory

An inventory of all computer and equipment and software will be maintained. It is the responsibility of each department manager or their named representative to detail each item of computer related equipment and software purchased, or disposed of, to the Computing Services. This department will keep a copy of the inventory and will periodically audit software that is installed. This policy will enable differences over time to be seen and then accounted for.

10.3 Software Register

An up to date register of all proprietary software will be maintained to ensure that Synrgise Learn is aware of its assets and that licence conditions are followed. This register will normally be maintained by Computing Services. System managers are responsible for informing Computing Services about the purchase of any software and that this purchase conforms to Synrgise Learn financial regulations.

11 Access control to secure areas

11.1 Objective

To minimise the threat to Synrgise Learn's computer systems through damage or interference.

11.2 Physical security

All central processors/networked file servers/central network equipment will be located in secure areas with restricted access.

Synrgise Learn's central computer suite will be a high security area housing corporate computer systems. An entry restriction and detection system will be incorporated to protect the suite.

Local network equipment/file servers and network equipment will be located in secure areas and where appropriate within locked cabinets.

11.3 Entry controls

Unrestricted access to the central computer facilities will be confined to designated Employees whose job function requires access to that particular area/equipment. Restricted access may be given to other Employees where there is a specific job function need for such access.

Authenticated representatives of third party support agencies will only be given access through specific authorisation.

All secure areas will have an entry log which Employees and visitors must use.

Regular reviews of who can access these secure areas should be undertaken.

12 Security of Third Party Access

12.1 Objective

To enable Synrgise Learn to control external access to its systems.

12.2 Access control

No external agency (will be given access to any of Synrgise Learn's networks unless that body has been formally authorised to have access. All non Organization agencies will be required to sign security and confidentiality agreements with Synrgise Learn.

Synrgise Learn will control all external agencies access to its systems by enabling/disabling connections for each approved access requirement.

Synrgise Learn will put in place adequate policies and procedures to ensure the protection of all information being sent to external systems. In doing so, it will make no assumptions as to the quality of security used by any third party but will request confirmation of levels of security maintained by those third parties. Where levels of security are found to be inadequate, alternative ways of sending data will be used.

All third parties and any outsourced operations will be liable to the same level of confidentiality as Organization Employees

13 User Access Control

13.1 Objective

To control individual's access to systems to that required by their job function.

13.2 Access to Systems

Employees and contractors should only access systems for which they are authorised. Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation. All contracts of employment, conditions of contract for contractor access agreements should have a non disclosure clause, which means that in the event of accidental unauthorised access to information, the member of Employees, contractor is prevented from disclosing information which they had no right to obtain.

13.3 Eligibility

The following are eligible to register as users:

- any person holding a contract of employment with Synrgise Learn;
- any person recommended by the Head of Department.

With the exception of access to material intended for the general public, use of information systems and networks shall be restricted to registered users.

13.4 Registering users

Formal procedures will be used to control access to systems. An authorised manager must countersign each application for access.

Access privileges will be modified/removed - as appropriate - when an individual changes job/leaves.

Each application for access should be countersigned by the manager against the rules agreed by the Head of Information Compliance & Policy.

13.5 User password management

A password is "Confidential authentication information composed of a string of characters" used to access computer systems.

Passwords must be kept confidential. Passwords are the responsibility of individual users; they must not be used by anyone else even for a short period of time. The giving of an authorised password to someone unauthorised in order to gain access to an information system may be a disciplinary offence. All system managers will ensure their systems enforce password changes at monthly intervals. A 12 month history of passwords should be kept.

Passwords must be at least 9 characters in length. They should be a mix of upper and lowercase and use other characters such as # @ \$ * etc. It is good practice to use 'screensaver' passwords in multiple occupancy offices, and essential in public areas. Passwords should be changed at least monthly, new systems should force this.

No Employees should be given access to a live system unless properly trained and made aware of their security responsibilities.

13.6 Employees leaving Synrgise Learn's employment

When a member of Employees leaves the employment of Synrgise Learn, their email account record is ended as part of the termination action carried out by HR on the SAP database. Computing Services run a SAP report based on this information and ensure that all email accounts for members of Employees no longer with Synrgise Learn are terminated.

Prior to an employee leaving, or to a change of duties, line managers should ensure that:

- the employee is informed in writing that he/she continues to be bound by their signed confidentiality agreement
- passwords are removed or changed to deny access
- relevant departments are informed of the termination or change, and, where appropriate, the name is removed from authority and access lists
- supervisors passwords allocated to the individual should be removed and consideration given to changing higher level passwords, to which they have access
- reception Employees and others responsible for controlling access to appropriate premises, are informed of the termination, and are instructed not to admit in future without a visitors pass
- where appropriate, Employees working out notice are assigned to non-sensitive tasks, or are appropriately monitored
- departmental property is returned

Particular attention should be paid to the return of items which may allow future access. These include personal identification devices, access cards, keys, passes, manuals & documents.

The timing of the above requirements will depend upon the reason for the termination, and the relationship with the employee. Where the termination is mutually amicable, the removal of such things as passwords and personal identification devices may be left to the last day of employment. Once an employee has left, it can be impossible to enforce security disciplines, even through legal process. Many cases of unauthorised access into systems and premises can be traced back to information given out by former employees.

System managers will delete or disable all identification codes and passwords relating to members of Employees who leave the employment of Synrgise Learn on their last working day. Prior to leaving, the employee's manager should ensure that all PC files of continuing interest to the business of Synrgise Learn are transferred to another user before the member of Employees leaves.

It is good practice for an 'exit' interview to be held during which the manager notes all the systems to which the member of Employees had access and informs the relevant system managers of the leaving date. Special care needs to be taken when access to patient identifiable data, personnel data and commercially sensitive and financial data is involved.

Managers must ensure that Employees leaving Synrgise Learn's employment do not inappropriately wipe or delete information from hard disks. If the circumstances of leaving make this likely then access rights should be restricted to avoid damage to Organization information and equipment.

In certain circumstances to be evaluated on a case by case basis researchers may be provided with access to an email account after they have left the employment of Synrgise Learn for a limited time.

13.7 Visitors and Contractors

All visitors to Departments should have official identification issued by Synrgise Learn and their arrival and departure times recorded. If temporary passwords need to be issued to allow access to confidential systems these need to be disabled when the visitor has left. Visitors should not be afforded an opportunity to casually view computer screens or printed documents produced by any information system without authorisation.

There is a requirement for System managers to have a procedure in place for the secure control of contractors called upon to maintain and support computing equipment and software. The contractor may be on site or working remotely via a communications link. Computing Services will advise on the most suitable control.

13.8 The Internet

Employees who wish to use Organization computers and telephone equipment for Internet services must have their 'connection' approved by Computing Services.

13.9 User Access Review

User access will be reviewed quarterly by the supervisors and Security Officer to reapprove all users and their access to the Synrgise Learn resources and data systems. This review presumes that all access is explicitly denied unless re-authorized through this process.

The data owners, supervisors and Security Officer are required to verify that each account on the access list should remain active and the access permissions are current.

The Security Officer or supervisor must sign, date, and return the supervision and review access control form to the Security Team within 20 business days distribution. If the supervisor or Security Officer fails to return the list within 20 business days, then all account on the list will be suspended until the list is received.

14 Housekeeping

14.1 Objective

To maintain the integrity and availability of computer assets.

14.2 Data Backup

Data should be held on a network directory where possible, to ensure routine backup processes capture the data. Should information be held on a PC hard drive the PC "owner" is responsible for backups.

Data should be protected by clearly defined and controlled back-up procedures which will generate data for archiving and contingency recovery purposes.

Computing Services and all other systems managers should produce written backup instructions for each system under their management. The backup copies should be clearly labelled and held in a secure area. Procedures should be in place to recover to a useable point after restart of this backup. A cyclical system, whereby several generations of backup are kept, is recommended.

Archived and recovery data should be accorded the same security as live data and should be held separately preferably at an off-site location.

Archived data is information which is no longer in current use, but may be required in the future, for example, for legal reasons or audit purposes.

Recovery data should be sufficient to provide an adequate level of service and recovery time in the event of an emergency and should be regularly tested.

To ensure that, in an emergency, the back-up data is sufficient and accurate, it should be regularly tested. This can be done by automatically comparing it with the live data immediately after the back up is taken and by using the back-up data in regular tests of the contingency plan.

Recovery data should be used only with the formal permission of the data owner or as defined in the documented contingency plan for the system.

If live data is corrupted, any relevant software, hardware and communications facilities should be checked before using the back-up data.

This aims to ensure that back-up data is not corrupted in addition to the live data. An engineer (software or hardware) should check the relevant equipment or software using his/her own test data.

14.3 Equipment, Media and Data Disposal

If a machine has ever been used to process personal data as defined under the Protection of Personal Information Act or "in confidence" data, then any storage media should be disposed of only after reliable precautions to destroy the data have been taken. Procedures for disposal should be documented.

Many software packages have routines built into them which write data to temporary files on the hard disk for their own purposes. Users are often unaware that this activity is taking place and may not realise that data which may be sensitive is being stored automatically on their hard disk.

Although the software usually (but not always) deletes these files after they have served their purpose, they could be restored and retrieved easily from the disk by using commonly available utility software.

Therefore, disposal should only be arranged through the Computing Services Department who will arrange for disks to be wiped to US Department of Defence standards.

15 Software and Information Protection

15.1 Objective

To comply with the law on licensed products and minimise risk of computer viruses.

15.2 Licensed software

All users should ensure that they only use licensed copies of commercial software. It is a criminal offence to make/use unauthorised copies of commercial software and offenders are liable to disciplinary action. Each user should ensure that a copy of each licence for commercial software is held.

The loading and use of unlicensed software on Organization computing equipment is NOT allowed. All Employees must comply with the Copyright Act. This states that it is illegal to copy and use software without the copyright owner's consent or the appropriate licence to prove the software was legally acquired. Synrgise Learn monitors the installation and use of software by means of regular software audits; any breaches of software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary action under Synrgise Learn Disciplinary Policy.

15.3 Unauthorised Software.

Synrgise Learn will only permit authorised software to be installed on its PCs. Approval will be via Computing Services.

Synrgise Learn will require the use of specific general purpose packages (e.g., word-processing, spreadsheets, databases) to facilitate support and Employees mobility. Non approved packages should be phased out as soon as practicable unless there is a definable business use.

Where Synrgise Learn recognises the need for specific specialised PC products, such products should be registered with Computing Services and be fully licensed.

Software packages must comply with and not compromise Organization security standards.

Computers owned by Synrgise Learn are only to be used for the work of Synrgise Learn. The copying of leisure software on to computing equipment owned by Synrgise Learn is not allowed. Copying of leisure software may result in disciplinary action under Synrgise Learn Disciplinary Procedure. Computer leisure software is one of the main sources of software corruption and viruses which may lead to the destruction of complete systems and the data contained on them.

Educational software for training and instruction should be authorised, properly purchased, virus checked and loaded by Computing Services Employees or its authorised representatives. Where a software training package includes 'games' to enable the new user to practise their keyboard skills e.g. Windows, then this will be allowed as long as it does not represent a threat to the security of the system.

15.4 Virus control

Synrgise Learn seeks to minimise the risks of computer viruses through education, good practice/procedures and anti-virus software positioned in the most vulnerable areas.

Users should report any viruses detected/suspected on their machines immediately to Computing Services. No newly acquired disks from whatever source, are to be loaded unless they have previously been virus checked by a locally installed virus checking package.

Users must be aware of the risk of viruses from email, the and the internet. If in doubt about any data received please contact the Computing Services Department for anti-virus advice.

15.5 Time-out procedures

Inactive terminals should be set to time out after a pre-set period of inactivity. The time-out facility should clear the screen. In high risk areas the time-out facility should also close both application and network sessions.

A high risk area might be a public or external area outside the control of Organization security management. The time-out delay should reflect the security risks of the area.

Users should log off terminals or PCs when leaving them unattended. PCs or terminals should be secured by a key lock or equivalent control (for example, password access control) when not in use.

For high risk applications, connection time restriction should be considered. Limiting the period during which terminal connection to IT services are allowed reduces the window of opportunity for unauthorised access.

16 Equipment Security

16.1 Objective

To protect IT equipment against loss or damage and avoid interruption to business activity

16.2 Equipment sitting and protection

IT equipment must always be installed and sited in accordance with the manufacturers specification. Equipment must always be installed by, or with the permission of Computing Services.

Where appropriate environmental controls will be installed to protect central or key equipment. Such controls will trigger alarms if environmental problems occur. In such cases where equipment is sited in a secure area, only authorised entry will be permitted.

Smoking, drinking and eating will not be permitted in areas housing computer equipment. Users should refer to local policies.

16.3 Power supplies

Where appropriate all sites within Synrgise Learn will have either UPS or generator backup to the mains electricity supply.

16.4 Network Security

It is the responsibility of the Head of Technical Services to ensure that access rights and control of traffic on all Organization networks are correctly maintained. Access rights to networked applications will be controlled by system managers. The Head of Technical Services will control access to personal data held on networked servers.

Each System Manager has a responsibility for keeping the Head of Technical Services informed of their requirements. This will include the number and names of users, their access requirements in terms of times and locations, the activities requiring network support and the needs of the support contractors.

System Managers must keep the Head of Technical Services informed of new users requiring access and those users who no longer need access either through changing jobs or leaving the employment of Synrgise Learn.

It is the responsibility of the Head of Technical Services to ensure that data communications to remote networks and computing facilities do not compromise the security of Synrgise Learn systems.

All communications cabling will be arranged by Computing Services and cannot be authorised without their involvement.

16.5 Use of '3G modems' and other communications equipment

Synrgise Learn aims to employ suitable measures to reduce risks of damage and corruption to its computer equipment and systems. The use of '3G modems' in an unstructured, unplanned and uncontrolled way puts its networks and information at risk. Therefore any unauthorised modification to computers is prohibited and 'approved modems' may only be attached to personal computers not connected to any of Synrgise Learn's networks.

Personal computers and '3G modems' must be bought via Computing Services.

16.6 Portable & Hand-held Computing Equipment

Equipment, data or software must not be taken off-site by Employees without documented management authorisation. (Management may provide authorisation on a 'once only' basis as long as it is subject to regular review)

Portable computers must have appropriate access protection, for example passwords and encryption and must not be left unattended in public places.

Computer equipment is vulnerable to theft, loss or unauthorised access. Always secure laptop and handheld equipment when leaving an office unattended. When travelling, the high incidence of car theft makes it inadvisable to leave in cars or take them into vulnerable areas.

To preserve the integrity of data, frequent transfers must be maintained between portable units and the main Organization system. The portable unit must be maintained regularly and batteries recharged regularly.

Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times on or off Organization property. The equipment should only be used by Organization Employees to which it is issued. All of the policy statements regarding the use of software and games apply equally to users of portable equipment belonging to Synrgise Learn.

Users of this equipment must pay particular attention to the protection of, personnel data and commercially sensitive data. The use of a password to start work with the computer when it is switched on, known as a 'power on' password, is mandatory and all sensitive files must be password protected if encrypting the data is not technically possible. The new user will refer to the instruction book to learn how to apply these passwords or may make arrangements for basic training in the use of a portable computer.

Users of portable equipment away from Organization premises should check their car and home insurance policies for their level of cover in the event of equipment being stolen or damaged and take appropriate precautions to minimise risk of theft or damage. Employees who use portable computers belonging to Synrgise Learn must use them solely for business purposes otherwise there may be a personal Tax/National Insurance liability.

16.7 System Documentation

All systems should be adequately documented by the System manager and should be kept up to date so that it matches the state of the system at all times.

System documentation, including manuals, should be physically secured (for example, under lock and key) when not in use. An additional copy should be stored in a separate location which will remain secure, even if the computer system and all other copies are destroyed.

Distribution of system documentation should be formally authorised by the system manager.

System documentation may contain sensitive information, for example, descriptions of applications processes, authorisation processes.

17 Incident Management

This procedure will be carried out in the event of any incident affecting the security of Personal Data or our Information systems as a whole.

In any case, the actions described in sections "17.1 Incident Communication", "17.2 Incident Recording" and "17.3 Incident Evaluation" will be carried out and the actions described in section "17.4. Notification of the Incident" in cases where the security incident poses a high risk to the rights and freedoms of those affected.

17.1 Incident Communication

- All staff are obliged to report any security incidents relating to personal data and security to the support desk. This notification will be made through the email address isec@Synrgise Learn.co.za or through the form placed at the corporate website.
- Incidents may occur in all activities related to the handling and management of information in physical format or logical databases that store personal data, as well as in the development of activities that affect the security of the data contained therein

The following are some examples of incidents:

- Collect personal data without the consent of the data subject and without informing him/her of his/her rights.
- Attempted or violated physical access control and databases.
- Alter databases (deletion, modification or inclusion of data that may affect the quality of the database).
- Removing data from media without proper authorization.
- Extract data on media other than those authorized in the database record.
- Failure to comply with the provisions of the Security Document for data recovery.
- Failure to comply with the deadlines established to resolve and respond to requests to exercise the rights of the interested party.
- Illegally using personal data.
- Execute the data recovery process.
- Improperly manage backups.
- Loss of tangible assets (work phone, laptops, etc.).
- Inability to access the system with our usual username/password.
- Possibly compromised access password.
- Abnormal system behaviour (incomplete or unrealistic information, unexpected failures, etc.).

Incidents relating to personal data are not limited to automate processing, but also include means of non-automated processing. Therefore, incidents affecting such media, such as the loss of paper lists containing personal data, must also be reported and recorded by the system described in this section.

17.2 Incident Registration

Once the security incident has been reported, the following actions will be taken:

- The Security Officer will formally record the security incident. In this regard, at least the following information shall be detailed:
 - Type of Incident.
 - Description of the Incident.
 - Date and time of the notification.
 - User reporting the incident.
- If necessary, the Security Officer will coordinate with the Information Security Manager to analyse the security incident. In addition, the Security Officer may request technical support from department heads during the analysis phase of the incident.

17.3 Incident Evaluation

Once the security incident has been recorded, the following actions will be performed:

- The Security Officer will evaluate the security incident.
- In the event that the Security Officer deems it appropriate, based on the criticality of the incident, he or she may call a meeting of the Security Committee in order to evaluate the impact of the incident on the group.
- The category or level of criticality of the incident with respect to the security of the affected information. Following the generic classification, we can distinguish between:
 - Critical (affects valuable data, large volume and in a short time)
 - Very High (When you have the capacity to affect valuable information, in appreciable quantity)
 - High (When you have the capacity to affect valuable information)
 - Medium (When you have the capacity to affect an appreciable volume of information)
 - Low (Little or no capacity to affect an appreciable volume of information).

In addition, there may be technical scenarios that may lead to an incident:

- 0-day (unknown vulnerability): Vulnerability that allows an attacker to access data to the extent that it is an unknown vulnerability. This vulnerability will be available until the manufacturer or developer resolves it.
- APT (targeted attack): This refers to different types of attacks that are normally aimed at gathering fundamental information that will allow the continuation of more sophisticated attacks. This category includes, for example, an email campaign with malicious software to employees of a company until one of them installs it on their computer and provides a gateway to the system.

- Denial of Service (DoS/DDoS): It consists of flooding a system with traffic until it is not able to provide service to its legitimate users.
- Access to Privileged Accounts: The attacker gets access to the system through a user account with advanced privileges, which gives him freedom of action. Previously, the user name and password must have been obtained by some other method, such as a targeted attack.
- Malicious Code: Pieces of software whose purpose is to infiltrate or damage a computer, server, or other network device for a variety of purposes. One of the possibilities for malicious code to reach an organization is for a user to unintentionally install it.
- Compromise of Information: Collects all incidents related to access and leakage, modification or deletion of non-public information.
- Data theft and/or filtration: Included in this category is the loss/theft of storage devices with information.
- Defacement: It is a type of directed attack that consists of the modification of the corporate website with the intention of posting messages of any kind or any other intention. The normal operation of the website is interrupted, causing reputational damage.
- Exploitation of application vulnerabilities: When a potential attacker successfully exploits an existing vulnerability in a system or product by compromising an organization's application.
- Social Engineering: These are deception-based techniques, usually carried out through social networks, which are used to direct a person's behavior or obtain sensitive information. For example, the user is induced to click on a link by thinking it is the right thing to do.

If any of these events happens to occur, the security incident must be reported:

- Any local data protection regulator.
- The affected parties

17.4 Incident Notification

17.4.1 Notification to the Supervisory Authority

As mentioned above, as soon as the data controller becomes aware that a breach in the security of personal data has occurred, he must, without delay and no later than 72 hours after becoming aware of it, make the corresponding notification to the Supervisory Authority. A security breach is considered to be recorded when there is a certainty that it has occurred and there is sufficient knowledge of its nature and scope.

The criterion to be taken into account in determining whether an incident has produced "a breach in the security of personal data" is included in the GDPR itself, and includes "all those security breaches that cause the accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or the unauthorized communication of or access to such data.

Identifying and contact data of:

- Entity / Person responsible for processing
- Data Protection Officer (if designated) or contact person
- Indication of whether the notification is complete or partial. In the case of a partial notification, indicate whether it is a first notification or a supplementary notification.

Information about the personal data security breach

- Date and time of detection.
- Date and time of the incident and its duration
- Circumstances in which the personal data security breach has occurred (e.g. loss, theft, copying, etc.)
- Nature and content of the personal data.
- Summary of the incident that caused the personal data security breach (with indication of physical location and storage medium).
- Possible consequences and negative effects on those data subjects affected.
- Technical and organizational measures taken by the controller
- Category of data affected and number of records affected.
- Category and number of individuals affected.
- Possible issues of a cross-border nature, indicating the possible need to notify other supervisory authorities.
- If, at the time of notification, it is not possible to provide all the information, it may be provided at a later stage, gradually in different stages. The first notification shall be made within 72 hours, and at least one final or closing communication shall be made when all the information relating to the incident is available.
- When the data controller makes the first notification, he or she shall state whether he or she will provide further information a posteriori. He may also provide additional information by means of intermediate communications to the supervisory authority at its request, or when the data controller considers it appropriate to update the situation of the supervisory authority.
- Where initial notification is not possible within 72 hours, the notification shall also be made a posteriori and shall state and justify the reasons for the delay.
- Notifications must be clear, concise and include the information necessary for them to be properly analysed.

17.4.2 Identification of the Supervisory Authority

Where an incident may affect the data of persons in more than one Province/State/Country, the controller should make an assessment of which is the main authority to which the notification should be made and, in case of doubt, at least notify the local supervisory authority where the breach has taken place. It will act as the main supervisory authority, the main establishment or the sole establishment of the person responsible.

The criteria for identifying the main establishment are:

- The place where the main headquarter of the data responsible is located.
- The place where decisions about ends and means are made.

17.4.3 Notification to the Data Subjects Concerned

As in the previous section, in the event of a security incident that poses a high risk to the rights and freedoms of those data subjects concerned, this should be communicated to the affected parties in order to enable them to take measures to protect themselves from the consequences of the incident.

The Security Officer is responsible for notifying the affected parties of the incident and must inform them of it within a reasonable period of time.

The notification will be made by email and will include the following information:

1. Contact details of the Security Officer, or where appropriate, the contact point where further information can be obtained.
2. General description of the incident and when it occurred.
3. The possible consequences of the personal data security breach.
4. Description of personal data and information affected.
5. Summary of measures implemented so far to control possible damage.
6. Other useful information to those affected to protect their data or prevent possible damage.

17.4.4 Exception to notification/communication

Notification to the Supervisory Authority will not be necessary where the data controller can demonstrate, in a reliable manner, that the breach in the security of personal data does not pose a risk to the rights and freedoms of natural persons.

For example, if the data were already publicly available and their disclosure does not entail any risk to the data subject.

Furthermore, communication to data subjects will not be necessary where:

- The responsible has taken appropriate technical and organizational measures, such as data not being intelligible to unauthorized persons or machines prior to the personal data security breach (through the use of: state-of-the-art data encryption, minimization, data dissociation, access to test environments without real data, etc.)
- For example, notification may not be necessary if a mobile device is lost and the personal data it contains is encrypted. However, notification may be required if this is the only copy of the personal data, or for example, the encryption key in the possession of the data controller is compromised.
- The data controller has taken protection measures that fully or partially mitigate the possible impact on those affected and ensure that there is no longer any possibility of the high risk materialising. For example, by immediately identifying and implementing measures against the person who has accessed personal data before they could do anything with it.
- When notification to those affected involves a disproportionate effort at the technical and organizational level. For example, where contact details have been lost as a result of the breach, or where a new notification system or process needs to be developed, or where excessive internal resources are required to identify data subjects concerned. In this situation, notification will be made publicly through the channels established by the data controller.

18 Electronic Mail (Email) Policy

18.1 Policy

Synrgise Learn provides employees with access to a variety of information technology systems and electronic communication media including Email for the pursuance of Organization business.

18.2 Care in drafting Emails

Users are responsible for drafting all emails carefully, taking into account any form of discrimination, harassment, Organization representation, and defamation of Data Protection issues.

Employees Emails are a form of corporate communication and therefore should be drafted with the same care as letters. Before sending proof read to make sure your message is understandable and appropriate. Do not send sensitive or emotional emails. If you are angry re-read it after you have calmed down. Never draft an email solely using CAPITALS – use normal sentence case.

Users should be careful when replying to emails previously sent to a group.

18.3 Viruses and Attachments

Employees are responsible for virus checking any attachment received before opening.

18.4 Information Confidentiality

Email is an insecure method of communication with content easily copied, forwarded or archived. Sensitive data should not be sent by this means.

18.5 Intent to enforce and monitor

Synrgise Learn reserves the right to carry out monitoring exercises on its systems, possibly without prior notice. Monitoring, via email blocking software may be used to block and read any email on Synrgise Learn network at any time by Synrgise Learn.

18.6 Retention and Purging

Deletion of old emails must be managed by each individual user, keeping in mind storage levels, archival levels, contractual evidence and legal discovery issues.

18.7 Junk mail

Email should not be sent to large numbers of people unless you are sure that it is directly relevant to their job. Sending unsolicited mail to many users ('spamming') is wasteful of user time and can disrupt the service, via performance delays, for other users.

18.8 Very large files

Sending of large files should be avoided where possible. The use of appropriately licensed compression software (e.g. *.zip files) is advised. Extremely large files should be sent by means other than email.

18.9 Protection of your terminal

Where terminals are left open and logged in when you leave your desk, a malicious user could send messages in your name. Ensure your terminal is locked or logged out.

18.10 Mail Storms

Avoid 'Mail Storms' – long discussions sent to a distribution list – consider verbal communication.

19 Client and Corporate Record Storage & Transportation

19.1 Objective

To identify and counter possible threats to Synrgise Learn's Records and determine protocols for their storage and transportation.

19.2 Storage

19.3 Offices

All Employee, Financial, Research and Corporate Records should be stored in a secure area and not left in an unattended, unlocked room. They should only be retained for the minimum length of time that they are absolutely required.

19.4 Elsewhere

All other areas where Records are stored should follow general the best practice guidelines of:

- Stored in a secure area
- Not left unattended
- Not kept for longer than necessary

19.5 Transportation

Where it is necessary to transport Records around Organization sites, the individual is responsible for ensuring their security. Records should not be left unattended at any time. When being transported by car records should be stored in a concealed area.

19.6 Responsibility

All Organization Employees who use, or come into contact with confidential records are individually responsible for their safekeeping. Employees should be aware of their contractual and legal confidentiality obligations.

20 Home working Information Security Standards

20.1 Objective

To provide Employees with information about the standards that should be used when they are working at home using computers (privately or Organization owned) and data. This can be a confusing area and it is necessary to ensure that Employees are informed and confident that they are doing the right thing.

Today's technology allows a number of options about the way we work. Synrgise Learn will continually study these options and develop appropriate protocols.

20.2 Authorisation to remove data files

Formal written authorisation by your Line Manager is required before person-identifiable data files can be taken home. Each Line Manager must inform the Head of Information Compliance & Policy of all Employees who regularly work with information at home. The Head of Information Compliance & Policy will maintain a register.

20.3 Transfer of personal data files

Person identifiable data files must not be sent via email to a user's home mail box. The Information (Data Protection) Commissioner has advised that Internet mail is not secure and should not be used to transmit confidential information.

20.4 Protecting data files

All electronic files used at home must be protected at least by file level password control.

20.5 Use of Privately owned Computers at Home

General Internet access carries with it a security risk of downloading viruses or programs that can look around a network and infiltrate password security systems. This information can then be sent back to the originator of the program in order to allow them unauthorised access to our systems. Therefore you must use care when transferring data between your home PC and Organization network. All home PCs which are used for the manipulation of Organization data must have a current virus checker.

20.6 Transportation of data or confidential documents

You should take reasonable care to minimise that risk of theft or damage, IT equipment must be transported in a clean, secure environment. During transfer of equipment between home and work you should keep the equipment out of sight and not leave it unattended at any time. Computer equipment or manual data must not be left in your car overnight.

20.7 Storage of equipment

You should take all reasonable steps to minimise the visibility of computer equipment from outside the home, and to secure windows and doors when the home is unoccupied.

20.8 Storage of confidential data or reports

You should secure confidential data or reports that you are not actively using in the most secure area of your home.

21 Appendix A: The Policy Review Process

Security policy documents should be living documents, changing & evolving as the organization and technology changes. Policies must undergo periodic review to ensure they are kept up to date. The final policy you publish is the one that will establish the review process that will incorporate the information collected as part of enforcement.

21.1 Periodic reviews of policy documents

- There is no rule as to how often the policy document is reviewed. However, it is suggested that it be reviewed bi-annually. This can be adjusted to suit the organization need
- The provision of the review process should include the ability to create an ad hoc review committee when there is an immediate requirement for a significant change to the policy.

21.2 What the policy review should include

- The information collected during the editing process will continue to be valuable
- Data collected while enforcing the policies and procedures that were created as a result of these policies
- Information collected from a risk assessment or audit
- Management can bring the business process and business intelligence as input
- Even hearsay information as to how everyone feels about the policies and resulting procedures can yield important information

21.3 The review committee

- Ideally, the review committee will consist of representatives from all stakeholders affected by the policies. These are the same stakeholders that were involved in editing the policy
- Smaller organizations may not be able to commit resources necessary to do review. These organizations can try creative methods rather than organizing meetings.

22 Appendix B: Antivirus Guidelines

22.1 What is a Virus?

A computer virus is a damaging piece of software that can be transferred between programs or between computers without the knowledge of the user. When the virus software is activated (by incorporated instructions, e.g. on a particular date), it performs a range of actions such as displaying a message, corrupting software, files and data to make them unusable, and deleting files and/or data. While many of the viruses produced are benign and cause no real damage to the infected system, they always constitute a breach of security.

There are currently something like 60-75,000 known viruses and worms - some 10-20 new viruses or variants appear a day. When a virus or worm is released into the public domain, network worms and mass mailer viruses can sometimes spread worldwide before anti-virus vendors have had time to produce updates.

Even daily anti-virus updates are not always enough to ensure safety from all possible threats.

22.2 What does Synrgise Learn do to prevent the spread of viruses?

Whilst precautions are taken at the network level to minimise the spread and impact of worms and viruses, it is not possible to make the process totally effective. Protection from viruses and worms is not a process that can be left entirely to system administrators, security officers, and anti-virus software. The best efforts of administrators and security experts are not sufficient - all computer users must also play their part by taking simple precautions like those described below.

22.3 Avoid Unauthorised Software

Programs like games, joke programs, cute screensavers, and unauthorised utility programs and so on can sometimes be the source of difficulties even if they are genuinely non-malicious. That is why it is forbidden for to install them. If such programs are claimed to be some form of antivirus or anti-Trojan utility, there is a high risk that they are actually in some way malicious!

22.4 Treat All Attachments with Caution

It makes sense to be cautious about email attachments from people you don't know. However, if attachments are sent to you by someone you do know, don't assume they must be OK because you trust the sender. Worms generally spread by sending themselves without the knowledge of the person from whose account they spread. If you do not know the sender or are not expecting any messages from the sender about that topic, it is worth checking with the sender that they intended to send a message, and if so, whether they intended to include any attachment. If you were expecting an attachment from them, this may not apply. However, one recent virus sends out an email telling you that a "safe" attachment is on the way, then sends out mail with a copy of itself as an attachment.

Bear in mind that even legitimate, expected attachments can be virus infected: worms and viruses are related, but cause slightly different problems.

Regard anything that meets the following criteria with particular suspicion:

If they come from someone you don't know, who has no legitimate reason to send them to you.

- If an attachment arrives with an empty message.
- If there is some text in the message, but it doesn't mention the attachment.
- If there is a message, but it doesn't seem to make sense.
- If there is a message, but it seems uncharacteristic of the sender (either in its content or in the way it's expressed).
- If it concerns unusual material like pornographic web-sites, erotic pictures and so on.
- If the message doesn't include any personal references at all, (for instance a short message that just says something like "You must take a look at this", or "I'm sending you this because I need your advice" or "I love you!").
- If the attachment has a filename extension that indicates a program file (such as those listed below).
- If it has a filename with a "double extension", like FILENAME.JPG.vbs or FILENAME.TXT.scr, that may be extremely suspicious. As far as Windows is concerned, it's the last part of the name that counts, so check that against the list below to find out whether it's a program like those listed, masquerading as a data file, such as a text file or JPEG (graphics) file.

In all the above instances, it is recommended that you check with the sender that they knowingly sent the mail/attachment in question.

22.5 Avoid Unnecessary Macros

If Word or Excel warn you that a document you're in the process of opening contains macros, regard the document with particular suspicion unless you are expecting the document and you know that it's supposed to contain macros. Even then, don't enable macros if you don't need to. It may be worth checking with the person who sent it to you that it is supposed to contain macros.

22.6 Be Cautious With Encrypted Files

If you receive an encrypted (password) attachment, it will normally be legitimate mail from someone you know, sent intentionally (though the sender is unlikely to know in the event that they have a virus). However, that doesn't necessarily mean that it isn't virus-infected. If it started out infected, encryption won't fix it. Furthermore, encrypted attachments can't usually be scanned for viruses in transit: the onus is on the recipient to be sure the

decrypted file is checked before it's opened. This goes not only for heavyweight encryption packages, but also for files compressed and encrypted with PKZip or WinZip.

22.7 Suspicious Filename Extensions

The following is a list of filename extensions that indicate an executable⁴ program, or a data file that can contain executable programs in the form of macros. This list is by no means all-inclusive. There are probably a couple of hundred filename extensions that denote an executable program of some sort. Furthermore, there are filenames like .RTF that shouldn't include program content, but sometimes can, while Word documents (for instance) can in principle have any filename extension, or none. Furthermore, zipped (compressed) files with the filename extension .ZIP can contain one or more of any kind of file.

.BAT	.CHM	.CMD	.COM	.DLL	.DOC	.DOT
.EXE	.FON	.HTA	.JS	.OVL	.PIF	.SCR
.SHB	.SHS	.VBS	.VBA	.WIZ	.XLA	.XLS

23 Appendix C: Risk Assessment Template

The risk assessment template is available on the company intranet and is laid out as per the below 'sample' screenshot.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	Risk ID	Risk	Asset owner	Impact	Raw probability	Raw impact	Raw risk rating	Treatment	Treatment cost	Treatment status	Treated probability	Treated impact	Treated risk rating	Current risk rating	Notes	Last update
2	12/10	Insider incident	GH	An insider exploits their access to steal, modify or delete information	88%	66%	58%	Oversight, logging, alarms and alerts	R 1 000,00	50%	87%	85%	74%	68%	WORKED EXAMPLE! This information is entirely fictitious.	2019/09/01
3	12/4	Global warming	GH	Extreme weather events	75%	66%	50%	Carbon tax	R 1 000,00	50%	10%	66%	7%	28%	WORKED EXAMPLE! This information is entirely fictitious.	2019/09/01
4	12/9	Melware	GH	Identity theft, exfiltration/theft of sensitive information, data corruption, ICT service outages	95%	35%	33%	Antivirus, security awareness, backups	R 450,00	50%	35%	40%	10%	22%	WORKED EXAMPLE! This information is entirely fictitious.	2019/09/01
5	12/6	New information security or privacy obligations introduced by laws and regulations etc.	GH	Noncompliance penalties	75%	44%	33%	Alertness for new compliance obligations	R 200,00	90%	10%	44%	4%	7%	WORKED EXAMPLE! This information is entirely fictitious.	2019/09/01
6	12/3	Earthquakes, tsunamis, eruptions	GH	Devastation of the immediate area, some environmental damage	50%	20%	10%	Business continuity arrangements	R 500,00	80%	50%	5%	3%	4%	WORKED EXAMPLE! This information is entirely fictitious.	2019/09/01
7	12/8	Spam	GH	Wasted resources, overload, diversion	100%	15%	15%	Spam filtering, security awareness	R 300,00	90%	5%	10%	1%	2%	WORKED EXAMPLE! This information is entirely fictitious.	2019/09/01
8	12/2	Small meteor striking Earth	GH	Devastation of the immediate area	25%	5%	1%	Share in an international ballistic missile defense system	R 5 000,00	0%	25%	1%	0%	1%	WORKED EXAMPLE! This information is entirely fictitious.	2019/09/01
9	12/1	Large meteor striking Earth	GH	Devastation of the immediate area, severe environmental damage	1%	100%	1%	Share in an international interplanetary ballistic missile	R 10 000,00	0%	0%	20%	0%	1%	WORKED EXAMPLE! This information is entirely fictitious.	2012/09/01
		Introduction	Risk register	Worked example	Guidance on usage	Guidance on scoring	+									

23.1 Guidance on usage

Column	Notes
ID	Assign a unique reference in order to be able to identify each risk unambiguously (e.g. "12/27" might be the 27th information security risk introduced into the analysis during 2012). Sequential numbers allow the table to be sorted sensibly!
Risk	Describe the information security risk briefly so that people will understand what risk you are assessing.
Asset owner	Who is the Information Asset Owner , the person who will be held to account if the risk treatments are inadequate, incidents occur and the organization is adversely impacted? It is in this person's interest to assess and treat the risks adequately, or face the consequences.
Impact	Describe the potential impacts should the risk occur, ideally in business terms. Decide whether to use "worst case" or "anticipated" impacts and be consistent about it! Consistency is especially important as the risk register gets larger and more people get involved in the assessments.
Raw probability	Enter the probability or likelihood that the risk would occur if it was totally untreated, as a percentage value (see the guidance on scoring).
Raw impact	Enter the potential business impact if the risk occurred without any treatment, as a percentage value (see the guidance on scoring).
Raw risk rating	This is the product of the raw probability and impact values, in other words the raw/untreated/inherent level of risk.
Risk treatment	Describe how the risk is to be treated. Note that controls are just one option: risks can also be avoided, transferred or accepted.
Treatment cost	Estimate the total cost of mitigating the risk.
Treatment status	To what extent is the planned treatment in place? 0% means the treatment is only a plan at present - nothing has been done about it as yet. 100% means the treatment is <i>fully operational</i> .
Treated probability	Enter the probability that the risk will eventuate once the controls etc. are fully in effect, in the same way as for before mitigation (see the guidance on scoring). Treated values are shown in bold if they are different to the raw values.

Information Security Policy Synrgise Learn

Treated impact	Enter the likely impact once the controls etc. are fully in effect, in the same way as before mitigation (see the guidance on scoring). Note that the impact of any incidents that actually do occur may INCREASE with strong controls in place, since incidents due to control failures are not usually expected. Treated values are shown in bold if they are different to the raw values.
Target risk rating	This is the product of the anticipated probability and impact values once the risk treatment is fully implemented.
Current risk rating	This is the risk rating today, given the implementation status and anticipated probability and impact values when fully completed. For example, if the raw risk value is 50% and the treated risk value is 30% but the treatment is only 50% implemented, the current risk level is 40%. In reality, many security controls are either fully implemented and fully effective, or partially implemented and not at all effective - but the risk calculation here takes into account the fact that work is under way, hence management can assume it will be treated in due course.
Notes	Keep notes about the risks e.g. the factors you have taken into account and your reasoning, including any significant assumptions.
Last checked	Record the date on which the risk was last reviewed, updated and/or approved by management. Sort on this column to find risks that have not been checked in a long time and hence maybe should be reviewed or reconfirmed.
	Note: you can sort the entire table on any column by clicking the triangle on the column heading. An arrow shows which column was last used.
	Make sure the conditional formatting is correctly colouring the risk ratings: it should be defined as a "colour scale" using 3 colours (green, amber and red) corresponding to the values 0%, 50% and 100%

23.2 Guidance on scoring

			Business impact				
			Extreme	Major	Moderate	Minor	Insignificant
			Complete operational failure, "bet the farm" impact, unsurvivable	Severe loss of operational capability, highly damaging and extremely costly but survivable	Substantial operational impact, very costly	Noticeable but limited operational impact, some costs	Minimal if any operational impact, negligible costs
			100%	80%	62%	25%	1%
(Almost) certain	We are <i>bound</i> to experience further incidents of this nature - in fact they are probably occurring right now!	100%	100%	80%	62%	25%	1%
Probable	We are likely to experience incidents of this nature before long	80%	80%	64%	50%	20%	1%
Possible	It is distinctly possible that we will experience incidents of this nature	62%	62%	50%	38%	16%	1%
Unlikely	Incidents of this nature are uncommon but there is a genuine chance that we may experience them at some future point	25%	25%	20%	16%	6%	0%
Rare	Although they are conceivable, we will probably never experience incidents of this nature	1%	1%	1%	1%	0%	0%

Note: the colors are generated automatically using Excel's conditional formatting.

The values assigned to each category are *arbitrary* so don't obsess about them: concentrate the need to mitigate those unacceptable red/amber risks!

24 Appendix D: IT Change Management Policies and Procedures

24.1 Introduction

- 24.1.1.1 Operational change management brings discipline and quality control to IS. Attention to governance and formal policies and procedures will ensure its success. Adopting formalised governance and policies for operational change management delivers a more disciplined and efficient infrastructure. This formalisation requires communication; the documentation of important process workflows and personnel roles; and the alignment of automation tools, where appropriate. Where change management is nonexistent, it is incumbent on IS's senior management to provide the leadership and vision to jump-start the process. By defining processes and policies, IS organisations can demonstrate increased agility in responding predictably and reliably to new business demands.
- 24.1.1.2 Synrgise Learn (hereafter called 'the company') management has recognised the importance of change management and control and the associated risks with ineffective change management and control and have therefore formulated this Change Management and Control Policy in order to address the opportunities and associated risks.

24.2 Scope

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

24.3 Purpose

- 24.3.1.1 The purpose of this policy is to establish management direction and high-level objectives for change management and control. This policy will ensure the implementation of change management and control strategies to mitigate associated risks such as:
- Information being corrupted and/or destroyed;
 - Computer performance being disrupted and/or degraded;
 - Productivity losses being incurred; and
 - Exposure to reputational risk.

24.4 References and definitions

24.5 Normative references

24.5.1.1 The following documents contain provisions that, through reference in the text, constitute requirements of this policy. At the time of publication, the editions indicated were valid. All standards and specifications are subject to revision, and parties to agreements based on this policy are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

- Information Security Policy (overall)
- Information Security - Systems Development and Maintenance Policy
- Information Security - Business Continuity Management
- Information Security - Physical Asset Classification and Control Policy
- Information Security – Change Control Procedure

24.6 Definitions and abbreviations

24.6.1 Audit trail

24.6.1.1 A record or series of records which allows the processing carried out by a computer system to be accurately identified, as well as verifying the authenticity of such amendments.

24.6.2 Information resources

24.6.2.1 All data, information as well as the hardware, software, personnel and processes involved with the storage, processing and output of such information. This includes data networks, servers, PC's, storage media, printer, photo copiers, fax machines, supporting equipment, fall-back equipment and back-up media.

24.6.3 Abbreviations

- **PC:** Personal Computer
- **BCP:** Business Continuity Plan
- **SLA:** Service Level Agreement

24.7 Policy

24.8 Preamble

24.8.1.1 Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.

24.8.1.2 In order to fulfil this policy, the following statements shall be adhered to:

24.8.2 Operational Procedures

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

24.8.2.2 At a minimum the change control process should include the following phases:

- Logged Change Requests;
- Identification, prioritisation and initiation of change;
- Proper authorisation of change;
- Requirements analysis;
- Inter-dependency and compliance analysis;
- Impact Assessment;
- Change approach;
- Change testing;
- User acceptance testing and approval;
- Implementation and release planning;
- Documentation;
- Change monitoring;
- Defined responsibilities and authorities of all users and IT personnel;
- Emergency change classification parameters.

24.8.3 Documented Change

24.8.3.1 All change requests shall be logged whether approved or rejected on a standardised and central system. The approval of all change requests and the results thereof shall be documented.

- 24.8.3.2 A documented audit trail, maintained at a Business Unit Level, containing relevant information shall be maintained at all times. This should include change request documentation, change authorisation and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorised personnel.

24.8.4 Risk Management

- 24.8.4.1 A risk assessment shall be performed for all changes and dependant on the outcome, an impact assessment should be performed.
- 24.8.4.2 The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.

24.8.5 Change Classification

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

24.8.6 Testing

- 24.8.6.1 Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made. (For more information see System Development Life Cycle [citation here]).

24.8.7 Changes affecting SLA's

- 24.8.7.1 The impact of change on existing SLA's shall be considered. Where applicable, changes to the SLA shall be controlled through a formal change process which includes contractual amendments.

24.8.8 Version control

- 24.8.8.1 Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies. (For more information see System Development Life Cycle [citation here])

24.8.9 Approval

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

24.8.10 Communicating changes

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

24.8.11 Implementation

- 24.8.11.1 Implementation will only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes. (For more information see System Development Life Cycle [citation here])

24.8.12 Fall back

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

24.8.13 Documentation

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

24.8.14 Business Continuity Plans (BCP)

- 24.8.14.1 Business continuity plans shall be updated with relevant changes, managed through the change control process. Business continuity plans rely on the completeness, accuracy and availability of BCP documentation. BCP documentation is the road map used to minimise disruption to critical business processes where possible, and to facilitate their rapid recovery in the event of disasters.

24.8.15 Emergency Changes

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

24.8.16 Change Monitoring

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

24.9 Roles and Responsibilities

ROLE	FUNCTIONAL RESPONSIBILITIES
Members of the Board	<ul style="list-style-type: none"> Members of the Board shall ensure that the necessary information security controls are implemented and complied with as per this policy.
Information Security Manager	<ul style="list-style-type: none"> Establish and revise the information security strategy, policy and standards for change management and control with input from interest groups and subsidiaries; Facilitate and co-ordinate the necessary counter measures to change management and control initiatives and evaluate such policies and standards; Establish the security requirements for change management and control directives and approval of the change management and control standards and change control/ version control products; Co-ordinate the overall communication and awareness strategy for change management; Acts as the management champion for change management and control; Provide technical input to the service requirements and co-ordinate affected changes to SLA's where applicable. Establish and co-ordinate appropriate interest group forums to represent, feedback, implement and monitor change management and control initiatives; and Co-ordinate the implementation of new or additional security controls for change management.
Operations Manager	<ul style="list-style-type: none"> Implement, maintain and update the change management and control strategy, baselines, standards, policies and procedures with input from all stakeholders; Approve and authorise change management and control measures on behalf of the Synrgise Learn; Ensure that all application owners are aware of the applicable policies, standards, procedures and guidelines for change management and control; Ensure that policy, standards and procedural changes are communicated to applicable owners and management forums; Appoint the necessary representation to the interest groups and

	<p>other forums created by each company for Information Security Management relating to change management and control;</p> <ul style="list-style-type: none"> • Establish and revise the information security strategy, policy and standards for change management and control; • Facilitate and co-ordinate the necessary change management and control initiatives within each company; • Report and evaluate changes to change management and control policies and standards; • Co-ordinate the overall communication and awareness strategy for change management and control; • Co-ordinate the implementation of new or additional security controls for change management and control • Review the effectiveness of change management and control strategy and implement remedial controls where deficits are identified; • Provide regular updates on change management and control initiatives and the suitable application; • Evaluate and recommend changes to change management/ version control solutions; and • Co-ordinate awareness strategies and rollouts to effectively communicate change management and control mitigation solutions in each company. • Establish and implement the necessary standards and procedures that conform to the Information Security policy; • Responsible for approving, authorising, monitoring and enforcing change management initiatives and related security controls within all Synrgise Learn companies and divisions; • Ensure that all solution owners are aware of policies, standards, procedures and guidelines for change management and control. • Ensure the compliance of this policy and report deviations to the Information Manager.
IT Service Provider	<ul style="list-style-type: none"> • Shall comply with all change management and control statements of this policy.
Solution Owners	<ul style="list-style-type: none"> • Shall comply with all information security policies, standards and procedures for change management and control; and • Report all deviations.

Table 1 Roles and Responsibilities

24.10 Compliance

24.10.1.1 Any person, subject to this policy, who fails to comply with the provisions as set out above or any amendment thereto, shall be subjected to appropriate disciplinary or legal action in accordance with the Synrgise Learn Disciplinary Code and Procedures. Company Information Security policies, standards, procedures and guidelines shall comply with legal, regulatory and statutory requirements.

24.11 IT Governance Value statement

24.11.1.1 Changes that materially affect the financial process must be evaluated and reported quarterly. Financial system upgrades or replacements will require new certification. The implication is that Sarbanes-Oxley compliance is reliant on the changes you make to the operational systems and procedures.

24.12 Policy Access Considerations

24.12.1.1 Access to this policy shall be granted to:

- All IT personnel
- Business Unit Management teams
- Executive Directors

25 Glossary & Abbreviations

For the purposes of this document the following definitions apply:

Access control the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorised manner.

Accountability the property that will enable the originator of any action to be identified.

Asset owner individual or organisation having responsibility for specified information assets and for the maintain of appropriate security measures.

Audit trail data collected and potentially used to facilitate any reconstruction of events in a system.

Authentication corroboration of the origin and correctness of any part of the system.

Authorisation the granting of rights which includes the granting of access based on access rights.

Availability information is delivered to the right person, when it is needed.

Confidentiality data access is confined to those with specified authority to view the data.

Data Owner the person who internal to the organization determines the purpose for which the information is to be used.

Data user means a person who holds data. A person holds data if:

The data forms part of a collection of data processed or intended to be processed by or on behalf of that person and that person either alone or jointly or in common with other persons controls the contents and use of the data comprised in the collection and the data are in the form in which they have been or are intended to be processed and with a view to being further so processed on a subsequent occasion

Degauss to remove unwanted magnetic fields and effects from magnetic disks, tape or read/write heads

Denial of service the prevention of authorised access to resources or the delaying of time critical operations

Impact the embarrassment, harm, financial loss, legal or other damage which could occur in consequence of a particular security breach

Information Security protection of information for confidentiality, integrity and availability

Integrity all system assets are operating correctly according to specification and in the way that the current user believes them to be operating

IT Information Technology

Password confidential authentication information composed of a string of characters

PC Personal Computer

Personal Data data consisting of information which relates to a living individual who can be identified from that information (or from that and other information in possession of the Data User), including any expression of opinion about the individual but not any indication of the intentions of the Data User in respect of that individual

[Data Protection Act (1998)]

Person Identifiable Data Any of the following items:

Surname, forename, initials, address, postcode, date of birth, other dates, sex, NI number, ethnic group, and occupation

Recovery restoration of a system to a desired state following a failure in the operation of the system.

Risk the likelihood of occurrence of a particular threat, with the degree of vulnerability to that threat and the potential consequence of that impact if the threat occurs.

Risk assessment comprehensive concept for defining and assessing the potential impact of threats, and vulnerabilities of, system assets and capabilities, and for supplying management with information suitable for a (risk management) decision in order to optimise investment in security counter measures.

Security breach any event that has, or could have, resulted in loss to Organization assets, or action that is in breach of Organization security procedures

Security Policy a statement of the set of rules, measures and procedures that determine the physical, procedural and logical security controls imposed on the management,

distribution and protection of assets and information

Threat an action or event which might prejudice security

Sensitivity a measure of importance assigned to information to denote its confidentiality

System Manager the person who determines the purpose(s) for which the system is to be used.

System Owner the person charged with the technical administration of the computer system.

Vulnerability a security weakness

26 References

This policy is based on the guidelines given in the following reference documents. However Employees with specific responsibility for Information Security may wish to refer to the source documents.

1. The Protection of Personal Information Act
2. ISO27000