Simfoni Information and Application Security Policy

SIMFONI

APPS AND ANALYTICS FOR OPERATIONAL IMPROVEMENT

DOCUMENT CONTROL				
VERSION	**CHANGE**	**AUTHOR**	**APPROVER**	**DATE**
0.1	New document following migration onto AWS infrastructure	E. Reshetov S Venkitakrishnan	P Allouche	03.05.16
1.0	Approved document	E. Reshetov S Venkitakrishnan	P Allouche	26.05.16
1.1	Network security	E. Reshetov	P Allouche	14.06.16
1.1.1	Network security additional comments	E. Reshetov	C Shah	12.07.16
1.3	Security protocol	E. Reshetov	C Shah	28.09.16
1.4	Programming standards	S Venkitakrishnan	C Shah	13.12.16
1.5	Data hosting Security protocol standards	S Venkitakrishnan	C Shah	06.04.17
1.5.1	Source code management	S Venkitakrishnan	C Shah	20.07.17
1.6	Password protection	S Venkitakrishnan	S Dent	05.12.17
1.7	Network security	S Venkitakrishnan	S Dent	04.01.18
1.9	Encryption Update	S Venkitakrishnan	S Dent	19.03.18
2.0	Policy review and update 2018	S Venkitakrishnan	S Dent	09.04.18
2.1	Edits to Data Handling and Hosting standards	S Venkitakrishnan	S Dent	17.07.18
2.2	Added Release procedure	S Venkitakrishnan	S Dent	26.09.18
2.3	Data encryption	S Venkitakrishnan	S Dent	26.12.18
2.4	Audit process	S Venkitakrishnan	S Dent	21.02.19
2.5	Minor Language update	S Venkitakrishnan	S Dent	14.08.19
2.6	Access Management update	S Venkitakrishnan	S Dent	22.10.19
2.7	Data Classification policy	S Venkitakrishnan	Jason Stern	20.01.2020
2.8	Data Retention and Retention Policy – Separated	S Venkitakrishnan	Jason Stern	15.03.2020
2.9	Incident Response Policy	S Venkitakrishnan	Jason Stern	01.06.2020
3.0	Updates to the Usage policy	S Venkitakrishnan	Jason Stern	20.10.2020
3.1	Secure Software Development Lifecycle Policy	S Venkitakrishnan	Chirag Shah	27.10.2020
3.2	Data classification policy	S Venkitakrishnan	Jason Stern	10.11.2020
3.3	Addition of GDPR to the main Infosec document	S Venkitakrishnan	Jason Stern	25.11.2020

CONTENT

1 GENERAL INFORMATION SECURITY 5

1.1 General Information Security Policy 5

2 EMPLOYEE BACKGROUND VERIFICATION POLICY 6

3 PROPRIETARY INFORMATION 6

3.1 Introduction 6

4 ACCEPTABLE USE POLICY 7

4.1 Overview 7

4.2 General Use and Ownership 7

4.3 Security and Proprietary Information 8

i. All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy. 8

ii. System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited. 8

iii. All computing devices must be secured with a password-protected screensaver. Company users must lock the screen or log off when the device is unattended. 8

iv. Postings by employees from a Simfoni email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Simfoni, unless posting is in the course of business duties. 8

v. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware. 8

4.4 Unacceptable Use 8

4.5 System and Network Activities 8

4.6 Email and Communication Activities 9

4.7 Blogging and Social Media 10

4.8 Compliance Measurement 10

4.9 Exceptions 10

4.10 Non-Compliance 10

5 PASSWORD PROTECTION 10

5.1 Password protection guidelines: 10

6 DISASTER RECOVERY AND BUSINESS CONTINUITY 11

6.1 Disaster recovery and business continuity policy 11

7 BREACH RESPONSE PROCEDURE 12

7.1 Scope 12

7.2 Process 12

7.3 Action plan 12
7.4 Close out actions 13
8 DATA AND SYSTEMS AUDIT 13
8.1 Audit management and delivery 13
9 APPLICATION SECURITY CONTROLS 14
9.1 Scope and Purpose 14
9.2 Network security 14
9.3 Data handling 14
9.4 Access Management 15
9.5 Encryption 15
9.6 Release Management 15
10 DATA CLASSIFICATION POLICY 17
10.1 Purpose 17
10.2 Scope 17
10.3 Data Classification 17
10.4 Data Collections 18
10.5 Reclassification 18
11 DATA RETENTION AND DESTRUCTION POLICY 20
11.1 Purpose 20
11.2 HOW LONG SHOULD WE RETAIN OUR RECORDS? 20
11.3 DISPOSAL SCHEDULE 20
11.4 SHARING OF INFORMATION 21
11.5 MONITORING 21
12 CLEAR DESK POLICY 22
12.1 Purpose 22
12.2 Scope 22
12.3 Policy 22
Clear Desk 22
13 INCIDENT RESPONSE POLICY 23
13.1 Security Incident Response Policy 23
13.2 Purpose 23
13.3 Scope 23
13.4 Incident Response Plan 23
13.5 Plan Testing 24

13.6 Notifying Third Parties 24
13.7 Data Breach 24
13.8 System Monitoring 24
14 SECURE SOFTWARE DEVELOPMENT LIFECYCLE POLICY 25
14.1 Requirement Gathering and Analysis 25
14.2 Design 25
14.3 Development 25
14.4 Testing 25
14.5 Deployment 25
14.6 Maintenance 25
15 GDPR POLICY 26
15.1 Determine your role under GDPR 26
15.2 Prepare for data subjects exercising their rights 27
15.3 Check cross-border data flows 27
15.4 Demonstrate accountability in all processing activities 27
15.5 Appoint a data officer 27
Staying Current 27

1 GENERAL INFORMATION SECURITY

1.1 General Information Security Policy

Overview & Purpose

The purpose of the General Information Security Policy is to ensure that personal and corporate data pertaining to Simfoni and Simfoni clients and affiliates of Simfoni, which includes Simfoni subsidiaries is managed in accordance with good practice and relevant data privacy, data protection and security laws and regulations. Simfoni is committed to protecting Simfoni directors, employees, customers, business partners and the company from illegal or any other damaging actions by individuals, either knowingly or unknowingly.

This policy includes multiple policy components, which together set out the general practices and operating principles for the management of all forms of data together with the security measures that are required to protect Simfoni, our employees, our business partners and our customers. Each sub policy must be issued to and read and acknowledged by all Simfoni directors, employees, contractors and affiliates.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Simfoni business or to interact with internal networks and business systems, whether owned or leased by Simfoni, provided by a client, an employee, or a third party.

Simfoni directors, employees, contractors, consultants and other workers at Simfoni, including all personnel affiliated with third parties who are performing services on behalf of Simfoni are required to adhere to the policies and processes contained within this master data security policy document and local laws and regulation.

Implementation

Simfoni directors, employees, contractors, consultants, temporary, and other workers at Simfoni and its subsidiaries are responsible for exercising good judgement regarding the appropriate use of information, electronic devices, and network resources in accordance with Simfoni policies and operating standards, and local laws and regulations.

All Simfoni employees – fulltime or temporary are required to read and confirm acceptance of the policy. Amendments to the policy are to be issued to all directors and employees.

General

i. For security and network maintenance purposes, authorized individuals within Simfoni may monitor equipment, systems and network traffic at any time in accordance with the Data Management and Security Audit Policy.
ii. Simfoni reserves the right to audit networks and systems used to support the delivery of Simfoni products and services on a periodic basis to ensure compliance with this policy.
iii. Simfoni employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

iv. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Simfoni are prohibited.
v. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Simfoni or the end user does not have an active license is strictly prohibited.
vi. Accessing data, a server or an account for any purpose other than conducting Simfoni business, even if you have authorized access, is prohibited.
vii. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
viii. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
ix. It is prohibited to use any Simfoni computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
x. Circumventing user authentication or security of any host, network or account.
xi. Providing information about, or lists of, Simfoni's employees, Simfoni's clients, Simfoni's partners to parties outside Simfoni is prohibited.

2 EMPLOYEE BACKGROUND VERIFICATION POLICY

Background checks are to be conducted on all employees as part of the standard HR on-boarding process. Background checks are to include disclaimers and checks with the previous employer related to behaviour, disciplinary records and reason for leaving.

Any issues arising with employee background checks or with current employees should in the first instance be relayed to HR and the relevant regional director. Should an issue be reported then access to all forms or client data should be immediately restricted for the relevant staff member whilst the issue is investigated. The staff member will only be granted access to client data should the issue be cleared by HR and the Regional Director. Refer to the company HR policy handbook for more information.

3 PROPRIETARY INFORMATION

3.1 Introduction

Proprietary information includes all forms of data pertaining to Simfoni products and services and customer related data, which includes beta products.

i. Simfoni proprietary information stored on electronic and computing devices whether owned or leased by Simfoni, the employee, Simfoni's client or a third party, remains the sole property of Simfoni. Simfoni and its employees are committed through legal or technical means to ensure that proprietary information is protected.

ii. Simfoni client information stored on electronic and computing devices whether owned or leased by Simfoni, the employee, Simfoni's client or a third party, remains the property of Simfoni during the period of the contract with the client and until it is not. Simfoni and its employees are committed through legal or technical means that proprietary information is protected.

iii. Use or share Simfoni proprietary information is limited only to the extent it is authorized and necessary to fulfil your assigned job duties and not for any personal use.

4 ACCEPTABLE USE POLICY

4.1 Overview

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Internet browsing, and FTP, are the property of Simfoni Limited. These systems are only to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

The purpose of this policy is to outline the acceptable use of computer equipment and networks at Simfoni Limited which are intended to protect the employee and the company. Inappropriate use exposes Simfoni to risks including virus attacks, compromise of network systems and services, and legal issues.

Effective data security is a team effort involving the participation and support of every Simfoni employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

4.2 General Use and Ownership

I. Simfoni proprietary information stored on electronic and computing devices whether owned or leased by the company, the employee or a third party, remains the sole property of Simfoni.

II. You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Simfoni proprietary information.

III. You may access, use or share Simfoni proprietary information only to the extent it is authorized and necessary to fulfil your assigned job duties.

IV. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

V. For security and network maintenance purposes, authorized individuals within Simfoni may monitor equipment, systems and network traffic at any time, per the company's Audit Policy.

VI. Simfoni reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

VII. Customer ownership of the data is governed by clauses on the agreement with the customer.

4.3 Security and Proprietary Information

i. All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.

ii. System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

iii. All computing devices must be secured with a password-protected screensaver. Company users must lock the screen or log off when the device is unattended.

iv. Postings by employees from a Simfoni email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Simfoni, unless posting is in the course of business duties.

v. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.4 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Simfoni authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Simfoni owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.5 System and Network Activities

The following activities are strictly prohibited:

i. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Simfoni.

ii. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Simfoni or the end user does not have an active license is strictly prohibited.

iii. Accessing data, a server or an account for any purpose other than conducting Simfoni business, even if you have authorized access, is prohibited.

iv. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

v. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses etc.).

vi. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

vii. Using a Simfoni computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

viii. Making fraudulent offers of products, items, or services originating from any Simfoni account.

ix. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

x. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

xi. Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made.

xii. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

xiii. Circumventing user authentication or security of any host, network or account.

xiv. Introducing honeypots, honeynets, or similar technology on the Simfoni network.

xv. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

xvi. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

xvii. Providing information about, or lists of, Simfoni employees to parties outside Simfoni.

4.6 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

i. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

ii. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

iii. Unauthorized use, or forging, of email header information.

iv. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

v. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

vi. Use of unsolicited email originating from within Simfoni's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Simfoni's or connected via the company's network.

vii. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups.

4.7 Blogging and Social Media

i. Blogging by employees, whether using Simfoni's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Simfoni's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Simfoni's policy, is not detrimental to Simfoni's best interests, and does not interfere with an employee's regular work duties. Blogging from Simfoni's systems is also subject to monitoring.

ii. Simfoni's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Simfoni confidential or proprietary information, trade secrets or any other material covered by Simfoni's Confidential Information policy when engaged in blogging.

iii. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Simfoni and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging.

iv. Employees may also not attribute personal statements, opinions or beliefs to Simfoni when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Simfoni. Employees assume any and all risk associated with blogging.

v. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Simfoni trademarks, logos and any other Simfoni intellectual property may also not be used in connection with any blogging activity.

4.8 Compliance Measurement

Simfoni will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.9 Exceptions

Any exception to the policy must be approved by the team in advance.

4.10 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5 PASSWORD PROTECTION

System level and user level passwords must comply with the following minimum standards:

5.1 Password protection guidelines:

i. Passwords must contain a minimum of 8 digits and include two (2) special characters

ii. Passwords should be kept confidential and should not be shared.

iii. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
iv. Passwords for all Simfoni products, emails, client platforms and other electronic mediums must be changed at least once every 3 months.
v. Passwords stored electronically may not be stored in readable form where unauthorized persons might discover them.
vi. Passwords may not be written down and left in a place where unauthorized persons might discover them.
vii. All Simfoni or client provided laptop and other electronic devices must be password protected with an auto-lock feature within 10 mins of inactivity.
viii. Revealing your account password to others or allowing use of your account by others is strictly prohibited. This includes family and other household members when work is being done at home.

The above-mentioned guidelines are subject to audit and revision from a time to time basis. Any exception to the policy must be approved by one of the Regional Managing Directors of Simfoni. Violation of this policy may be subject to disciplinary action, up to and including termination of employment.

6 DISASTER RECOVERY AND BUSINESS CONTINUITY

Overview and Purpose

Simfoni management supports disaster contingency planning efforts as part of wider business contingency planning. A disaster means any event that could likely cause an extended delay of a core service. This policy outlines the guidelines to report an issue or loss, recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

6.1 Disaster recovery and business continuity policy

i. In any event of threats, inability to access or other technical challenges to the computers of the Simfoni employees which may disrupt client servicing or cause data loss/ damage must be immediately reported to Simfoni IT and Security Administrator.
ii. All Simfoni employees must be cross trained and succession plan created to avoid any loss of knowledge, data which may cause disruption or delay to client services.
iii. All, Simfoni internal or client, data storage must be reported and tracked using criticality and confidentiality.
iv. Criticality must be defined for all data, systems and processes so that in event of recovery, the critical ones are prioritized ahead of the less critical ones.
v. All data pertaining to client services which includes but not limited to client data provided for analysis or delivery of service, client user data, Simfoni process related data etc. must have back-up systems in place to avoid permanent loss.
vi. In case of any loss of data, Simfoni employees must contact relevant Product Manager to recover the data.
vii. In event of Business disruptions, Simfoni Regional Managing Directors and/or Client Account Leads are responsible to communicate the recovery and business continuity plan with the client engagement managers within 24 hours from the time of identification of disruption.

viii. Provision cross regional teams to act on behalf of the primary team in case of disruptions which cause regional disruptions to client services.

The above-mentioned guidelines are subject to audit and revision from a time to time basis. Any exception to the policy must be approved by one of the Regional Managing Directors of Simfoni. Violation of this policy may be subject to disciplinary action, up to and including termination of employment.

7 BREACH RESPONSE PROCEDURE

The Data Breach Response policy is focused on Simfoni's management of any perceived or actual data security breaches and how Simfoni should respond to such an occurrence. Simfoni Information Security is committed to protecting Simfoni's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

This policy mandates that any individual who suspects that a theft, breach or exposure of Simfoni Protected data or Simfoni's Sensitive data has occurred must immediately call the Regional Managing Director and provide a description of what occurred via e-mail to info@simfoni.com, with the Regional Managing Director on copy. This e-mail address is monitored by the Simfoni IT & Security Administrator. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Simfoni IT & Security Administrator will follow the appropriate procedure.

7.1 Scope

This policy applies to all directors, employees, contractors and agents involved who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Information of Simfoni and its clients. The scope includes data loss as well as data breach.

7.2 Process

As soon as a theft, data breach, loss or exposure has been reported, the Regional Managing Director will chair a response team to handle the breach or exposure. The team will involve the Simfoni IT & Security Administrator together with members from IT Development, IT Administration, Product Management, Legal, and Head of Departments from the affected operations.

The Regional Managing Directors are also responsible to communicate such events to each other and to the clients within 24 hours from the identification of the event and the action plan to mitigate the risk and to strengthen controls to avoid a future occurrence.

Upon confirmation of theft or breach, the Regional Managing Director may appoint forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyse the breach or exposure to determine the root cause.

7.3 Action plan

An action plan will be formulated with support from legal to decide how to communicate the breach to those directly affected which may include customers, employees and the general public, and what action is required to remedy the breach. The plan will be reviewed and approved by the appropriate Regional Managing Director(s).

7.4 Close out actions

Once the breach has been contained and addressed and the appropriate action taken to inform those parties affected then the Regional Managing Director(s) with the Simfoni IT and Security Administrator will close out the plan and document the cause and nature of the breach and the action taken for audit purposes.

8 DATA AND SYSTEMS AUDIT

This audit policy provides guidelines to the Simfoni team and directors regarding performing data security audits on IT infrastructure and systems used to host and manage data to ensure that the company is protected from security threats, which includes the following:

i. Access to confidential data
ii. Unauthorized access of the client data and computers
iii. Password disclosure compromise
iv. Virus infections
v. Intrusions and Denial of service attacks

8.1 Audit management and delivery

Audits may be conducted to: Ensure integrity, confidentiality and availability of information and resources

i. Monitor all security measures to ensure conformance Information Security Policies
ii. Investigate security incidents recorded in security log book

Simfoni will operate an appropriate system of internal audit, which provides an assessment of security policies. Internal audits are conducted two times a year. The Product Manager for each Simfoni product will be responsible for conducting an internal audit of security controls. When requested and for performing an audit, any access needed will be provided to members of any External Audit team. This access may include:

i. User level and/or system level access to any computing or communications device
ii. Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on respective Dept. equipment or premises
iii. Access to work areas (labs, offices, cubicles, storage areas, etc.)
iv. Access to interactively monitor and log traffic on networks.

9 APPLICATION SECURITY CONTROLS

9.1 Scope and Purpose

The purpose is to establish administrative direction, procedural requirements, and technical guidance to ensure the appropriate protection of Simfoni's information handled by cloud networks.

9.2 Network security

Network controls:

i. Limit access to cloud instances and software programs to authorized persons.
ii. Maintain logs of users with access to the cloud console, program repositories.
iii. Define a process for granting system privileges which includes access to read/ write/ edit programs are approved by one of the Regional Managing Directors
iv. Manage password protection in accordance with the defined password protection protocols.
v. Define and manage a process for revoking system access in place and maintained in the user log.
vi. Security controls should be in place to identify and alert on DoS and DDoS attacks, controls in place for Bot intrusions.
vii. Use of AWS WAF for protection against application-layer attack such as SQL injection and cross-site scripting.
viii. Use AWS Shield Advanced to protect the network and application against DDoS, DoS and other types of penetrations.

9.3 Data handling

Data security controls in place includes:

i. All Simfoni client documents and data loads are to be classified with version control – this includes contracts, agreements, emails, datasets etc.
ii. All data in Simfoni's cloud application(s) are to be encrypted using secure sockets layer (SSL).
iii. Simfoni's client data stored in the cloud data base is to be encrypted using Amazon EBS. Changing the encryption status of the data requires additional approval from Simfoni Regional Managing Director.
iv. Simfoni's client data is to be stored in separate schema or databases as required and separated from other client or internal data with appropriate controls.
v. Simfoni adheres to the guidelines set out below with respect to data retention and deletion:
    - All Simfoni data is retained for 3 years unless instructed otherwise by a Regional Managing Director.
    - All Simfoni client data is retained during the period of the contract and beyond unless specifically agreed for a disposal.
    - Data archives can only be accessed by authorised persons.
    - Data deleted from the client instances and from the cloud backend upon request from the or as agreed in the client contract.

- Back up – All client data hosted within Simfoni software or cloud should have a primary backup for the below mentioned items:
    - Usage log – Login by users, their session time etc.

- Changes and approval – All changes made to the data in the platform including approvals etc. to have a log maintained in the back up.
- Database backup – storing of data in the back up instances. Back-ups are to be taken every 24 hours with storage of the past 5 versions of the data.
- More frequent data back-up can be implemented on a client-by-client basis and approved by the Regional Managing Director.

9.4 Access Management

Controls are defined below which ensure that access to the platform, data and programs are limited to authorised users:

i. Access to all Simfoni software, cloud instances, source code repositories are approved by either a Head of Products or a Regional Managing Director.
ii. All approvals for authorized access to the Simfoni software, cloud instances, source code to be on email.
iii. List of users and their accesses to be maintained as a log and adding users, access privileges or revoking the same to be tracked in the log.
iv. No more than two persons can hold the super admin access which has all the controls.
v. All client user addition should be authorized by the client engagement manager or the sponsor via email.
vi. User logins allowed only with real email addresses and in-built with the password reset mechanism and confirmation of the account.
vii. Password protection to follow the guidelines of the General Information security policy.

9.5 Encryption

Data encryption minimum standards:

i. All passwords to be encrypted and managed using key management services.
ii. Data – at rest and in transit. Secure Sockets Layer for protection while in transit and server-side encryption using Amazon SSE- S3, 256-bit Advanced Encryption Standard (AES-256).
iii. Software source codes for client installation are to be encrypted using obfuscation technique.

9.6 Release Management

New products and update releases is managed in a structured manner for all Simfoni software and for all type of releases - be it a bug fix or feature release or a performance enhancement through code optimization. Simfoni's Head of Products is responsible for all the development related activities and risks and product and release management.

All releases will be scheduled and will consider the following:

i. Requirement risk assessment – An assessment of all risk pertaining to a specific development in a software. These risks to be assessed includes the impact to the existing features, data exposure, data security, authentication and controls.

ii. Specification documentation – Based on the nature of the development, a specification documentation to be prepared. This will be stored in a centrally managed issue logging system for tracking and future auditing purposes.

iii. Staged development and testing – developments must only happen within a development environment, tested in the staging environment and then only moved to production.

iv. Functional testing – All core features within all Simfoni software to have unit test coding covered and ready for automated quality assurance.

v. Functional Testing should cover areas including user paths, security loopholes, data sharing and exposure, data extraction, intrusion etc.

vi. Version history – version history of the source code is to be maintained to be able to revert to a previous version in case of accidental release.

10 DATA CLASSIFICATION POLICY

10.1 Purpose

The purpose of this policy is to establish a framework for classifying data based on its level of sensitivity, value, regulatory requirements, and criticality to the Simfoni, its employees and its customers. Classification of data will aid in determining baseline security controls for the protection of data.

10.2 Scope

This Policy applies to all employees, contractors, and third-party agents of Simfoni as well as any other partners who is authorized to access Simfoni's data.

Definitions

- **Data Stewards**: Simfoni senior management (typically at the level of Director) who oversee data management functions related to the capture, maintenance, and dissemination of data for an operational area. They are responsible for decisions about the usage of Simfoni data under their purview.
- Data Users: Individuals and organizations that access Simfoni data and Information to perform their assigned duties or to fulfil their role.
- Data: All Simfoni, its employees or its customer data.

10.3 Data Classification

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the Simfoni should that data be disclosed, altered, or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All data should be classified into one of three sensitivity levels, or classifications:

A) Restricted Data

Data should be classified as Restricted when the unauthorized disclosure, alteration, or destruction of that data could cause a significant level of risk to Simfoni or its affiliates. Examples of Restricted Data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to Restricted Data.

B) Private Data

Data should be classified as Private when the unauthorized disclosure, alteration, or destruction of that data could result in a moderate level of risk to Simfoni or its affiliates. By default, all Data that is not explicitly classified as Restricted or Public Data should be treated as Private Data. A reasonable level of security controls should be applied to Private Data.

C) Public Data

Data should be classified as Public when the unauthorized disclosure, alteration, or destruction of that data would result in little or no risk to Simfoni and its affiliates. Examples of Public Data include press releases, course information, and research publications. While little or no controls are required to protect the confidentiality of Public Data, some

level of control is required to prevent unauthorized modification or destruction of Public Data.

D) Confidential data

Data should be classified as Classified when a Private data needs to be shared with our customers. This data should be such that does not pose serious risk to Simfoni, other than possible loss of IP which could be reused. Hence the use of confidential classification.

An appropriate Data Steward should perform classification of data.

10.4 Data Collections

Data Stewards may wish to assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used. For example, if a data collection consists of a customers' name, address and personal contact information, the data collection should be classified as Restricted.

10.5 Reclassification

On a periodic basis, it is important to re-evaluate the classification of Data to ensure the assigned classification is still appropriate based on changes to legal and contractual obligations as well as changes in the use of the data. The appropriate Data Steward should conduct this evaluation. Conducting an evaluation on an annual basis is encouraged; however, the Data Steward should determine what frequency is most appropriate based on available resources. If a Data Steward determines that the classification of a certain data set has changed, an analysis of security controls should be performed to determine whether existing controls are consistent with the new classification. If gaps are found in existing security controls, they should be corrected in a timely manner, commensurate with the level of risk presented by the gaps.

Security Objective	Potential Impact		
	Low	**Medium**	**High**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11 DATA RETENTION AND DESTRUCTION POLICY

11.1 Purpose

Simfoni needs to gather and use certain information, and also process and store certain types of information to operate our business. These providers list include learners, members, customers, business contacts, suppliers, employees and other people the organisation has a relationship with and may need to contact. This policy describes procedures for the retention and disposal of information to ensure that we carry this out consistently and that we fully document any actions taken. Unless otherwise specified the retention and disposal policy refers to both hard and soft copy documents.

11.2 HOW LONG SHOULD WE RETAIN OUR RECORDS?

Records should be kept for as long as they are needed to meet the operational needs of Simfoni, together with legal and regulatory requirements. We have assessed our records to ascertain business use and any legal or regulatory obligations (including, but not limited to Data Protection Act 1988, The GDPR, and Limitation Act 1980 etc.). For certain records of a personal value to an individual, such as a certificate of achievement or award, we will retain them indefinitely.

11.3 DISPOSAL SCHEDULE

The disposal schedule (Appendix 1) lists collections or groups of records for which predetermined periods of retention have been ascertained. Records can be destroyed in the following ways:

- Non-sensitive information – can be placed in a normal rubbish bin
- Confidential information (including personal data belonging to customers or employees) – crosscut shredded and pulped or burnt.
- Electronic equipment or systems containing information - destroyed by IT and for individual folders/emails/database records, they will be permanently deleted from the system.
- Destruction of electronic records should render them non-recoverable even using forensic data recovery techniques.

Disposal Schedules

Business Function	Type of records	Retention Period
HR	Personnel files	5 years
	Application forms, Interview ads, redundancy documentation	6 months
Payroll	All	3 years
Health & Safety	Accident books, Health records	3 years
Insurance	General insurance	3 years
	Employee Liability Insurance	40 years
Financial records	Purchase	6 years

	Invoice	10 years
	Income	1 year
	Customer contracts	6 years

11.4 SHARING OF INFORMATION

Duplicate records should be destroyed. Where information is regularly shared between departments, only the original source records should be retained in accordance with our policies.

Where we share information with partners, contractors and other bodies, we will ensure they have adequate procedures to manage the information in accordance with the relevant legislation and regulatory guidance.

11.5 MONITORING

Responsibility for monitoring the data retention policy sits with the Senior Management Team (SMT). This policy will be reviewed on an annual basis.

12 CLEAR DESK POLICY

12.1 Purpose

The purpose of this policy is to reduce the risk of unauthorized access, loss and damage to information during the timeframe when workstations/laptops/servers are left unattended.

12.2 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Simfoni, including all personnel affiliated with third parties. This policy applies to all equipment (including mobile computing devices) that is owned, rented or leased by Simfoni Solutions.

12.3 Policy

Clear Desk

1. Paper, external mail and computer removable media shall be stored in suitable locked safes, cabinets. etc.
2. In case lockable safes, cabinets, drawers etc. are not available, entrance doors shall be locked, if left unattended. At the end of each work session, all sensitive information shall be removed from the workspace and stored in a safe place. This includes all business-critical information.
3. Sensitive or classified information should be removed from printers immediately.
4. The reception desk shall be kept clear at all times; in particular, personnel records, postal mails or other identifiable information should not be kept on a desk within reach/sight of visitors.

Clear screen

1. Computer terminals shall not be left unattended and shall be locked and password protected.
2. Screens shall be angled away from the view of unauthorized persons, if possible.
3. The log on dialog box shall be displayed if the system remains inactive for 15 minutes.
4. Users shall log off from their machines before leaving the premises.
5. Inappropriate access or viewing of the display screen of any computing device holding confidential information shall be minimized.

13 INCIDENT RESPONSE POLICY

13.1 Security Incident Response Policy

It is the policy of Simfoni that personnel must report all unusual and/or suspicious security-related events. These events may include unusual and troublesome requests for internal information coming from an external party, previously unseen dysfunctional system behaviour, suspected computer virus infections, erroneous system results, social engineering, and information service failures. All unauthorized disclosures of electronic data must be reported to the CEO in writing.

It is the policy of Simfoni that individuals must not attempt to deal with data security incidents, violations or problems without expert technical assistance. Technical responses to security incidents, violations and problems must be handled by the CEO and/or others who have been authorized by the CEO.

An Incident Response Plan shall be implemented and utilized for all suspicious security-related events.

13.2 Purpose

Regulations related to the unauthorized disclosure of electronic data require reporting and mitigation processes be established to address them in a timely manner. The purpose of this document is to define the relevant responsibilities and provide guidance for the management and response to computer security incidents and data breaches.

13.3 Scope

This document applies to all Simfoni personnel accessing or utilizing computer resources, data communication networks, or other information technology infrastructure resources owned or leased by Simfoni; including any other corporation having connectivity to the network.

13.4 Incident Response Plan

An Incident Response Plan must be implemented in the event of a system breach. The Incident Response Plan must contain incident response procedures, Information system service restoration procedures, incident response team responsibilities, status reporting requirements, post-incident assessment procedures, and documentation requirements. These procedures must document how to re-establish a trusted computing environment, as well as procedures to document the events so that post-mortem analyses can be performed.

The incident response plan addresses the following:

- Roles, responsibilities, and communication and contact strategies in the event of a compromise;
- Response times based on severity levels;
- Specific incident response procedures;
- Includes a response in the event an unauthorized wireless device is detected;
- Notification requirements;

- Business recovery and continuity procedures;
- Data back-up processes;
- Analysis of legal requirements for reporting compromises;
- Coverage and responses of all critical system components;
- Reference or inclusion of incident response procedures from the payment brands.
- The incident response plan includes a review / lessons learned process. Using information from completed incidents, modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

13.5 Plan Testing

At least once a year, the IT Engineering Team must utilize simulated incidents to mobilize any and all Corporate Team Members employees who have an active role and test the adequacy of the Incident Response Plan.

13.6 Notifying Third Parties

If a data breach causes private or proprietary third-party information to be exposed, then these same third parties must be promptly notified so that they can take appropriate action. All such external notification efforts must be approved by the CEO with information on the breach provided by the COO.

13.7 Data Breach

The term 'breach' means the unauthorized acquisition, use, or disclosure of electronic data which compromises the security or privacy of such information.

The term 'breach' does not include any unintentional acquisition, or use of electronic data by an employee or individual acting under the authority of a Service Provider if such acquisition, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the Service Provider; and such information is not further acquired, accessed, used, or disclosed by any person; Any inadvertent disclosure from an individual who is otherwise authorized to access sensitive information at a facility operated by a Service Provider to another similarly situated individual at same facility; and any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

The Incident Response Plan shall address all data breach and data breach notification requirements.

13.8 System Monitoring

Systems shall include alerts from intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.

14 SECURE SOFTWARE DEVELOPMENT LIFECYCLE POLICY

Before building any kind of application feature the developer(s) should know all the phases of our software development lifecycle. It will improve the development process and quality of the application. It consists of 5 phases to build an application as per the requirement in a cost-effective way. Each phase has its own process and it looks like cycle manner.

Here we have detail view about each phase.

14.1 Requirement Gathering and Analysis

Requirements describe the features of the system we are going to design, develop etc. This is a most crucial phase in the software development lifecycle. The Product head would plan out the feature and give the requirements. The Product head will share the requirement in a Jira ticket with the engineering team.

14.2 Design

In this phase, the developer given the task would take the input from the Product Head and design the architecture of the system/feature and document it.

14.3 Development

The developer(s) will do programmatic part here. This is the longest phase of the whole cycle. Developers will divide each module into different tasks and then will start coding/implementing each task. After completion of coding part, developers will do unit testing to find the logical errors in the initial stage.

At the time of unit testing, if developers find any major issue or enhancements regarding requirements, they will report to Product Head. After completion of this phase, the system will move to the testing phase.

14.4 Testing

The developer(s) will test all the modules developed in the previous phase as a complete system. The developer will do different kinds of test approaches to certify the application. Testing types are functional testing, system testing, regression, load testing, performance testing, UAT etc.

The developer(s) will write test cases for each module with the positive and negative scenarios. If they find any bugs at the time of testing, again the development process will take place. The module would be then deployed to test environment for testing.

14.5 Deployment

After fixing all the defects, the software will be deployed to production environment.

14.6 Maintenance

Once the software is deployed, it should be under maintenance for few days. Because in the user environment we may get errors at the time of functioning. We have to fix those issues to work the software in a smooth manner.

15 GDPR POLICY

Simfoni is committed to providing our Procurement technology to our Clients in compliance with applicable laws and regulations in general and data privacy laws such as the EU General Data Protection Regulation (GDPR) in particular.

What GDPR means to you?

Effective as of May 25, 2018 the GDPR will replace the currently applicable EU Data Protection Directive. Unlike the Data Protection Directive, the GDPR will have direct effect in all EU member states without any need for local implementing legislation and it will override existing national privacy laws.

Besides strengthening and standardizing user data privacy across the EU nations, the GDPR will require new or additional obligations on all organisations that handle EU citizens' personal data, regardless of where the organisations themselves are located.

Whenever the Data Protection Directive or the GDPR applies to our Clients they are deemed the controller of the personal data included on the Simfoni Platform and Simfoni is deemed the processor. As such, both Simfoni and our Client have to comply with their respective obligations under the Data Protection Directive and the GDPR accordingly. One side of these obligations relates to the controller processor relationship, while the other side relates to the controller obligations vis-à-vis the data subject, typically the user of the Simfoni Platform (i.e. employees, contractors and partners of our Clients).

We expect our Clients and their users to comply with all applicable laws and regulation in connection with the use of the Simfoni Platform, in particular making sure, that our Clients have all rights and consents necessary to allow Simfoni to use and process such data.

As a service provider, Simfoni is committed to supporting our Clients in their compliance activities, including as outlined in GDPR Chapter III (Rights of the data subject), most notably the rights of access and rectification (Art. 15 + 16 GDPR), right to erasure or 'right to be forgotten' (Art. 17 GDPR), right to data portability (Art. 20 GDPR), and right not to be subject to automated decision-making, including profiling (Art. 22 GDPR).

Our priorities

15.1 Determine your role under GDPR

As a cloud-based procurement technology provider, Simfoni is processing data on behalf of its Clients using the Simfoni Platform; therefore, Simfoni is seen as a data processor under the GDPR. In light of existing data privacy laws and data security measures generally expected from a global cloud service provider such as Simfoni, we have already implemented an information security program consisting of policies and procedures to help ensure that Simfoni is acting in accordance with current and new compliance requirements when providing our services.

15.2 Prepare for data subjects exercising their rights

Within the Simfoni Platform, our Clients use the personal data of their users to interact with each other in order to better manage their procurement processes. These acting individuals are the data subjects and our Clients - acting as data controllers - need to be able to answer certain legitimate requests under the GDPR. As such, our Clients will look to Simfoni as service provider and data processor to offer functionalities within the Simfoni Platform that enable our Clients to achieve compliance. Our internal product design processes are focused on the user and their positive and productive experience on the Simfoni Platform. In light of GDPR, Simfoni periodically reviews the Simfoni Platform features in order to validate that the Simfoni platform provides the required functionalities to our Clients.

15.3 Check cross-border data flows

Both the Data Protection Directive and the GDPR permit personal data transfers outside of the EU subject to compliance with defined conditions, including conditions for onward transfer. When a Client contracts with Simfoni, we can enter into a Data Processing Agreement (DPA) with applicable Clients. In the DPA, we agree with our Client on the terms for the compliant processing of Client personal data, including the description of our security and data privacy policy and the EU standard contractual clauses.

15.4 Demonstrate accountability in all processing activities

Simfoni's compliance program is already comprehensive and based on globally accepted standards. Simfoni has implemented an information security program consisting of policies and procedures that define how system information is entered, managed, and protected. Simfoni's current information security program is further specified in our Master Subscription Agreement (MSA) as well as our Data Processing Agreement (DPA). In particular, Simfoni commits to monitor, analyse and respond to security incidents in a timely manner in accordance with Simfoni's standard operating procedure, which sets forth the steps that Simfoni employees must take in response to a threat or security incident. Simfoni continues to invest in a growing global security capability.

15.5 Appoint a data officer

The GDPR will require some organisations to designate a Data Protection Officer (DPO). Organisations requiring DPOs include public authorities, organisations whose activities involve the regular and systematic monitoring of data subjects on a large scale, or organisations who process what is known as sensitive personal data on a large scale. At Simfoni, we have appointed a leadership team member to this role.

Staying Current

Ensuring the privacy and security of our Client's data is an ongoing commitment for Simfoni. We will continue to update this document to reflect any GDPR-related developments.