simplisys

Simplisys Security Policy

Version 1.5
Date: 4th Feb 2018

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk
www.simplisys.co.uk

Table of Contents

Introduction

This document defines the security policy in use at Simplisys

Acceptable Use Policy

The Simplisys acceptable use policy is defined in the document Simplisys Acceptable Use Policy that can be found on the company SharePoint site

http://vsql03/sites/Simplisys/Service%20Documentation/Acceptable%20Use%20Policy.docx

Backup Policy

Details of the SImplisys Backup policy are help in the backup policy document

Data Protection Policy

The Simplisys Data Protection policy is defined in the document Data Protection policy that can be found on the company SharePoint site

http://vsql03/sites/Simplisys/Service%20Documentation/Data%20Protection%20Policy.docx

Cryptography

Where data is of a sensitive personal nature or where unauthorised disclosure may cause significant harm to the company consideration should be given to encrypting the data in question.

Where data is to be encrypted only approved cyphers should be used.

Approved Cypher List

The following Cyphers are currently approved for use:

- Triple DES 169
- AES 128
- AES 256

Key Management

Creation

Encryption keys, Including Symmetric keys, Public. Private key pairs must be generated by the IT Security Manager, or where automatically generated by software authorised by the IT Security manager

All keys should be clearly labelled with their use, and validity dates

Protection

All encryption keys should be stored in sharepoint in the I.T. Security sub site. Access to this site to be restricted to IT Security manager, Development Manager and senior Company staff.

Data Classification Policy

2.1 Owners and Production Information

All electronic information managed by IS must have a designated Owner. Production information is information routinely used to accomplish business objectives. Owners should be at the VP level or above. Owners are responsible for assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. They are instead designated members of the *Simplisys* management team who act as stewards, and who supervise the ways in which certain types of information are used and protected.

2.2 RESTRICTED

This classification applies to the most sensitive business information that is intended for use strictly within *SIMPLISYS*. Its unauthorized disclosure could seriously and adversely impact *simplisys* its customers, its business partners, and its suppliers.

2.3 CONFIDENTIAL

This classification applies to less-sensitive business information that is intended for use within *Simplisys* . Its unauthorized disclosure could adversely impact *Simplisys* or its customers, suppliers, business partners, or employees.

2.4 PUBLIC

This classification applies to information that has been approved by *Simplisys* management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm.

2.5 Owners and Access Decisions

Data Owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. IS must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of electronic information.

Email Policy

The Simplisys Email policy is defined in the document Email Policy that can be found on the company SharePoint site

http://vsql03/sites/Simplisys/Service%20Documentation/Email%20Policy.docx

Guest Access Policy

Granting Guest Access

Guest access will be provided on a case-by-case basis to any person who can demonstrate a reasonable business need to access the network, or access the Internet from the company network.

AUP Acceptance

Guests must agree to and sign the company's Acceptable Use Policy (AUP) before being granted access.

Approval

Guest need for access will be evaluated and provided on a case-by-case basis. This should involve management approval if the request is non-standard.

Account Use

Guest accounts, if offered, are only to be used by guests. Users with network accounts must use their accounts for network access. Guest accounts must be set up for each guest accessing the company's network. Guest accounts must have specific expiration dates that correlate to the business need for the individual guest's access. The account expiration date is not to exceed thirty days.

Security of Guest Machines

Guest machines must be audited by the Information Technology department before being allowed to access the network. The company should ensure that that the Network Access Policy will be adhered to, which may involve a virus/malware scan prior to being granted access.

Restrictions on Guest Access

Guest access will be restricted to the minimum amount necessary. Depending on the guest needing access, this can often be limited to outbound Internet access only. The company will evaluate the need of each guest and provide further access if there is a business need to do so.

Monitoring of Guest Access

Since guests are not employees of the company they are not considered trusted users. As such, the company will monitor guest access to ensure that the company's interests are protected and the Acceptable Use Policy is being adhered to.

Incident Response Policy

Contacting the Simplisys Helpdesk

Anybody requiring support should call the Simplisys Helpdesk as below:

By Email: support@Simplisysservicedesk.com
By Fax: 01275 240501
By Post
Simplisys Ltd,
Portis Fields
15 Middle Bridge Business Park
Bristol Road
Portishead Bristol, BS20 6PN United Kingdom.
By Telephone: 01275 240500

IT Security Incidents

All actual or suspected IT Security Incidents should be reported at once to the IT Security manager.

The IT Security Manager will

- Perform an initial investigation to ascertain:
    - The nature of the event
    - This risk to Customer or company data
- Formulate an initial response plan
- Communicate the Incident details and Initial response plan to the senior Management Team
- Manage the implementation of the response plan

The senior Management Team will

- Communicate with any customer impacted
- Ensure that the ICO is informed if a data breach has happened

Priority Definitions and Turnaround Targets

Customers to indicate the impact of the incident related to their operation. Simplisys will then prioritise the urgency of the technical diagnosis and resolution turnaround. Simplisys will use best endeavours to meet the response target

'Service Levels' defined below.

- 'Response Target' is defined as the mean time to the first 'useful contact'.
- 'Workaround Target' is the time to the first available feasible solution.
- 'Resolution Target' is the time to the first available solution.

Customer Priority	Response	Workaround	Resolution	Contact / Action
1-Urgent **Product operation unusable. High customer business procedure at risk. A time-critical service unavailable.**	30 mins	2 hours	4 Hours	**SIMPLISYS CARE Helpdesk** Telephone/email initial response Hourly monitoring of progress Mandatory positive response required.
2-Major **Product component/important facility unusable. Software/data files not accessible. Time-critical service schedule endangered.**	30 mins	4 hours	16 Hours	**SIMPLISYS CARE Helpdesk** Telephone/Email initial response. Bi-daily monitoring of progress. Mandatory positive response required.
3-Default Level **Product/component will not run/job impaired. Workaround to problem has been found**	4 hours	1 day	5Days.	**SIMPLISYS CARE Helpdesk** Daily monitoring of progress Telephone/Email response.
4-Not to Spec **Product will not run as documented but issue is not critical – Bug Fix**	1 day	2 days	Next release.	**SIMPLISYS CARE Helpdesk** Weekly monitoring of progress Telephone/Email response.
5-Not Clear **Non-critical issues. E.g.;** **Documentation Errors, Usability suggestions, etc.**	1 day	5 days	No SLA	**SIMPLISYS CARE Helpdesk** Weekly monitoring of progress Telephone/Email response.

Simplisys Service Cover

Simplisys can provide service-cover to meet a customer’s support needs and this is defined within the contracted ‘Service

Maintenance Agreement’ outlined below: -.

‘Standard Service-Cover’ [5 x 9 hours]	08:30 to 17:30 hours Monday to Friday	Excludes all public holidays and week-ends
‘Extended Service-Cover’ [5 x 14 hours]	08:30 to 22:00 hours Monday to Friday	Excludes all public holidays and week-ends
‘Premier Service-Cover’ [7 x 8 hours]	8:30 to 17:30 hours Saturday, Sunday and all UK public holidays	Excludes Christmas Day and Boxing Day
‘Bespoke Service Cover’	Up to 7 x 24 as required.	To be agreed

Mobile Device Policy

SImplisys does not employ mobile devices

Network Access Policy

Introduction

This sets forth standards which must be adhered to by all employees, contractors and any user granted access to any machine on the Local Area Network (LAN) at any time, whether physically present at the Firm or via remote access.

Failure to comply with the policies set forth in this document will result in disciplinary action, and may result in termination of employment.

Logical Security

All computers and devices on the LAN must adhere to the other polices in this document and mentioned in this document

Physical Security

All computers and devices on the LAN must be physically secured when leaving them unattended. All servers must be additionally secured with locking devices such as keyboard locks.

Any notebook or laptop computer, Personal Digital Assistant (PDA), Internet-capable cellular device,

Wi-Fi-enabled device or other device capable of connecting via Remote Access to the LAN (A “Mobile Device”) must be secured with a BIOS password, and user authentication. Any Mobile Device must run up-to-date anti-virus protection and properly configured software firewall

Any Authorized User must take reasonable steps to ensure that any Remote Access to the LAN is treated with the same security approach as a connection made within the Firm..

Network Security Policy

Network Attached Equipment

Any devices attached to the simplisys production network MUST adhere to the following:

PCs

- Domain joined
- Patched to Patching standard
- Windows security essentials installed and set to auto update
- Firewall active (All Network types)

Patching Policy

The patching policy is to apply application and O/S patches within a month of their release. Critical security patches will be applied as soon as possible but always within 1 week of their release.

Where testing shows a patch may cause issues the deployment of the patch may be delayed with the authority of the IT Security manager. This authority must be reviewed every 7 days

Maintenance Schedule

Week	Server	Activity	Notes
1	Infrastructure Servers: Domain Controllers	Test Environment Patching	During week 1 patches are applied and tested on the test environments
1	End User Computing Devices	Test O/S Patching	
2	Infrastructure Servers: Domain Controllers	Production O/S Patching	
3	End User Computing Devices	Production O/S Patching	

Log Retention Policy

All logs are to be retained for a minimum of 90 days.

Where logs are, or may be, required for a longer period, for example to allow software debugging or incident investigation they may be retained until no longer required.

Logs that have been retained beyond the 90 day default period MUST be destroyed as soon as they are no longer required.

User Management Policy

Creation

New users need to read and sign a copy of the acceptable use policy.

Once received the user creation will be approved and the IT security manager will create the user in AD

Removal

As soon as an employee leaves employment or an account is no longer required, such as a service account no longer needed the account must be moved into the Disabled accounts OU and after 30 days deleted

Password Policy

Overview

Passwords must be used to protect access to all equipment and data used by Simplisys

Passwords MUST meet the following requirements

• Enforce password history	24 passwords remembered
• Maximum password age	42 days
• Minimum password age	1 days
• Minimum password length	7 characters

Where automatic lockout is available it MUST be implemented meeting following requirements

• Account lockout duration	30 minutes
• Account lockout threshold	5 invalid logon attempts
• Reset account lockout counter after	30 minutes

Passwords are never to be disclosed. If a password is forgotten a new password will be generated and applied.

Remote Access Policy

Remote access to simplisys systems MUST be agreed with the Security Manager before use

Remote Devices

Any Employee using any Remote Device must ensure that such device is updated with the most recent security patches for their Operating System.

All machines on the LAN and any Remote Device must run current versions of anti-virus software with regularly updated virus definitions. Note that new viruses are introduced every hour; “regularly updated virus definitions” means at a minimum of once each week. It could be argued it is reasonable to update every 24 hours.

Any Remote Device must be running a properly-configured firewall program such as Zone Alarm or Computer Associates eTrust. Users at Public Hotspot must be aware that, if such Remote Device is not running a firewall, a malicious user can gain access to the Remote Device and install software or remove files from the Remote Device’s hard drive.

No Firm email may be sent using third-party email services (including but not limited to gmail, hotmail, etc).

Any Authorized User accessing any computer or device on the LAN for remote management or administration must use Remote Desktop For remote file transfer, SCP, SFTP or VPN must be used. Under no circumstances shall Telnet, FTP or other un-encrypted access method be used.

No Employee using any Remote Device shall access the LAN while connected to any other network, except a personal network over which such Employee has complete control.

Wireless Policy

General Requirements

All wireless infrastructure devices that reside at a Simplisys site and connect to a Simplisys network, or provide access to information classified as Simplisys Confidential, or above must:

- *Abide by the standards specified in the* Wireless Communication Standard*.*
- *Be installed, supported, and maintained by an approved support team.*
- *Use Simplisys approved authentication protocols and infrastructure.*
- *Use Simplisys approved encryption protocols.*
- *Maintain a hardware address (MAC address) that can be registered and tracked.*
- *Not interfere with wireless access deployments maintained by other support organizations.*

Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to Simplisys Confidential or above, must adhere to the general requirements above. Lab and isolated wireless devices that do not provide general network connectivity to the Simplisys network must:

- *Be isolated from the corporate network (that is it must not provide any corporate*

connectivity) and comply with the Lab Security Policy.
- *Not interfere with wireless access deployments maintained by other support organizations.*

Home Wireless Device Requirements

Wireless infrastructure devices that provide direct access to the Simplisys corporate network, must conform to the Home Wireless Device Requirements as detailed in the *Wireless Communication Standard*.

Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the Simplisys corporate network. Access to the Simplisys corporate network through this device must use standard remote access authentication.

Policy Compliance

Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

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

Non-Compliance

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

Appendix A: Technical Controls

Active Directory

Active directory default domain policy is used to implement the following:

- Password Policy
- Automatic Lockout Policy