Security In Project Management Guide

PHX046

Contents

Background

Information security is required to be considered at all stages of a project lifecycle for projects within the business.

This document provides guidance on information security within project management across the relevant departments.

Project Management Type

The company deals with project management that fall into several categories, detailed below:

- Software Asset Management
- Consultancy Services
- Systems Development
- General Project Management

Documents

The following documents have been produced in order to ensure that all relevant parties understand how information security is considered within the project management lifecycle.

Software Asset Management

Introduction

This document has been produced to highlight the current Security Controls within projects completed in the Software Asset Management division. The SAM division's main deliverable is the Clarity Core – Managed Service.

The section below identifies the process along with security considerations and controls.

Managed Service

	Task Name
	Stage 1 - Project Initiation
1	Agree and sign off Statement of Works
2	Project Kick off call with customer
3	Project plan to create and share with customer
4	Request Letter of Authorisation

5	Complete Non-Disclosure/data sharing/ DPIA documents where appropriate
Task Name	
6	Accept all project documentation and sign off.
	Stage 2 - Inventory Tool Deployment
7	Deploy Inventory Tool to desktops
8	Deploy Scanwin to Servers
9	Implement Universal Data Agent
	Stage 3 - Data Extract
10	Extract from all customer inventory sources
11	Transfer's data via universal data or sftp site where appropriate
12	Coverage checks of devices/servers scanned
	Stage 4 – Software recognition service (SRS)
13	Identify unmatched software
14	Install summary and report sent to consultant
15	Import all data sets
	Stage 5 - License Inventory
16	Request License Evidence from Vendors
17	Import License Evidence
18	Automatically Allocate Base Licenses
19	QA Upgrades without base
	Stage 6 - Servers
20	Export Master server template
21	Review server template with client
22	Re-import server template
	Stage 7 - ELP
23	Auto allocate
24	Manual Check
25	Produce Draft ELP
26	Deliver SAM Report and ELP
	Stage 8 – Retention & Deletion
27	Customer data is retained in a secure location and then deleted when appropriate.

Security Considerations

Item 5 - Complete Governance Documentation

The Non-Disclosure agreement is a controlling document used to protect both parties throughout the duration of the contract.

A data sharing or data protection data impact assessment ensures all data is shared/stored and retained following the correct procedures and must be completed as appropriate.

Item 11 - Transfer's data to sftp site

During the Software Recognition Service stage data is transferred to Phoenix Software using universal data which is encrypted using HTTPS / TLS 1.2.

Secure file transfer protocol (sftp) is also used. Each user requires a password to gain access to this site. The password and link to the site are sent via email separately as per security best practice. Once this data has been uploaded the Support desk transfers this data to our internal data file system and deletes the data from the sftp. The internal data file system has restricted access so only authorised employees can gain access.

Item 16 - Request License Evidence from Vendors

During the license inventory stage we will request evidence of License purchases as part of the project. In order to request this data we require a signed letter of authorisation from the client (Item 4). This data is stored on a secure network drive which only the Software Asset Management Team have access to.

Item 26 - Deliver SAM Report and ELP

Once the ELP has been created we send this across to the client in PDF format. The document is marked 'Strictly Private and Confidential and is password protected. The password for the pdf is sent to the client in a separate email and is a once only password so if the password is lost a new one will be generated.

Item 27 – Retention and Deletion
All customer data is stored on a secure network drive and retained and deleted in line with Phoenix's retention policy. Details of retention and deletion is also written in the contract which the customer reviews, agrees, and signs off.

Consultancy Services

We offer our customers a consultancy service which take place on their sites or via remote access.

The Project Manager meets with each customer and works through a Project Initiation Meeting (PIM) and Project Initiation Document (PID). Details of their contents are below. Security aspects of the projects are discussed and Phoenix Software Ltd adhere to the agreed customer requirements. Further documentation is created and highlighted in bold below.

Project Initiation Meeting Agenda (PIM)

- Technical Design & Whiteboard Session
    - Networking

    - Infrastructure Services
    - Security and Compliancy
    - Client Services
    - Operations and Deliverables
    - Responsibilities and Pre-requisites
- Policies and Procedures
    - Change Control Process (Internal and 3rd Party)
    - User Acceptance Testing / Criteria
    - Security Policy
    - Access Management
    - Communication
- Risk Assessment and Management
    - Identify project risks

Project Initiation Documentation (PID)

- Document Purpose
- Disclaimers
- Project Approach and Scope
    - Details the deliverables per phase
- Milestones and Timescales
- Roles and Responsibilities
- Client Responsibilities
- Quality Control
- Change Control
- Risk, Issues and Escalation Process
- Project Tolerances
- Exception Process
- Exclusions
- Acceptance Note
- Appendices
    - Change Control Form
    - Issue Log
    - Risk Log

Project Plan

Project Management RAID Log

(NDA) between Phoenix Software Ltd and the customer where appropriate

Issue NDA to 3rd Party (if applicable)

Issue Contract Agreement to 3rd Party (if applicable)

Systems Development

A guide named "Systems Development Process Checklist" is held on SharePoint/System Development. The checklist includes prompts to discuss the level of security required within individual projects.

General

There are a wide variety of projects that take place within the business that may fall outside of the above parameters. These include but are not limited to - IT infrastructure changes, implementation of third-party software, building and repair work to Blenheim House, engagement with new vendors/technologies.

Information security should be addressed regardless of the type of project and the following taken into consideration:

- Security risks are identified and addressed e.g., data exposure to third parties, loss of customer data, levels of user access to confidential information, unauthorised access to the building, third parties viewing confidential data held around the building
- Information security objectives as listed in the Information Security Policy are included in project objectives
- Information security risk assessment is conducted at an early stage of the project to identify necessary controls
- Information security implications should be addressed and reviewed regularly in all projects
- The ISC are available to provide implementation guidance as required

An Information Security within Projects Template is to be used by all relevant employees and uploaded to SharePoint/Administration/ISO27001/Information Security within Projects. The ISC review these documents in their quarterly review meetings.

Version Control

Author	Version	Date	Description
Clare Metcalfe	1.0	20/11/2015	Document submitted
Clare Metcalfe/Mark Jay/Jason Davies	2.0	03/09/2018	Annual Review
Clare Metcalfe/Mark Jay/Jason Davies	3.0	01/04/2020	Annual Review
ISC	3.0	02/04/2021	Annual Review
ISC	4.0	18/07/2022	Amendments following annual review
Jonathan Buxey	5.0	29/06/2023	Annual review – SAM section expanded

Document Approval

Name	Version	Date	Position
Clare Metcalfe	1.0	20/11/2015	Operations Director
Clare Metcalfe/Mark Jay/Jason Davies	2.0	03/09/2018	PM's
Clare Metcalfe/Mark Jay/Jason Davies	3.0	01/04/2020	PM's
ISC	3.0	02/04/2021	ISC
Clare Metcalfe	4.0	18/07/2022	Operations Director
Clare Metcalfe	5.0	29/06/2023	Operations Director

Signed:  Clare Metcalfe, Operations Director

Dated: 29/06/2023