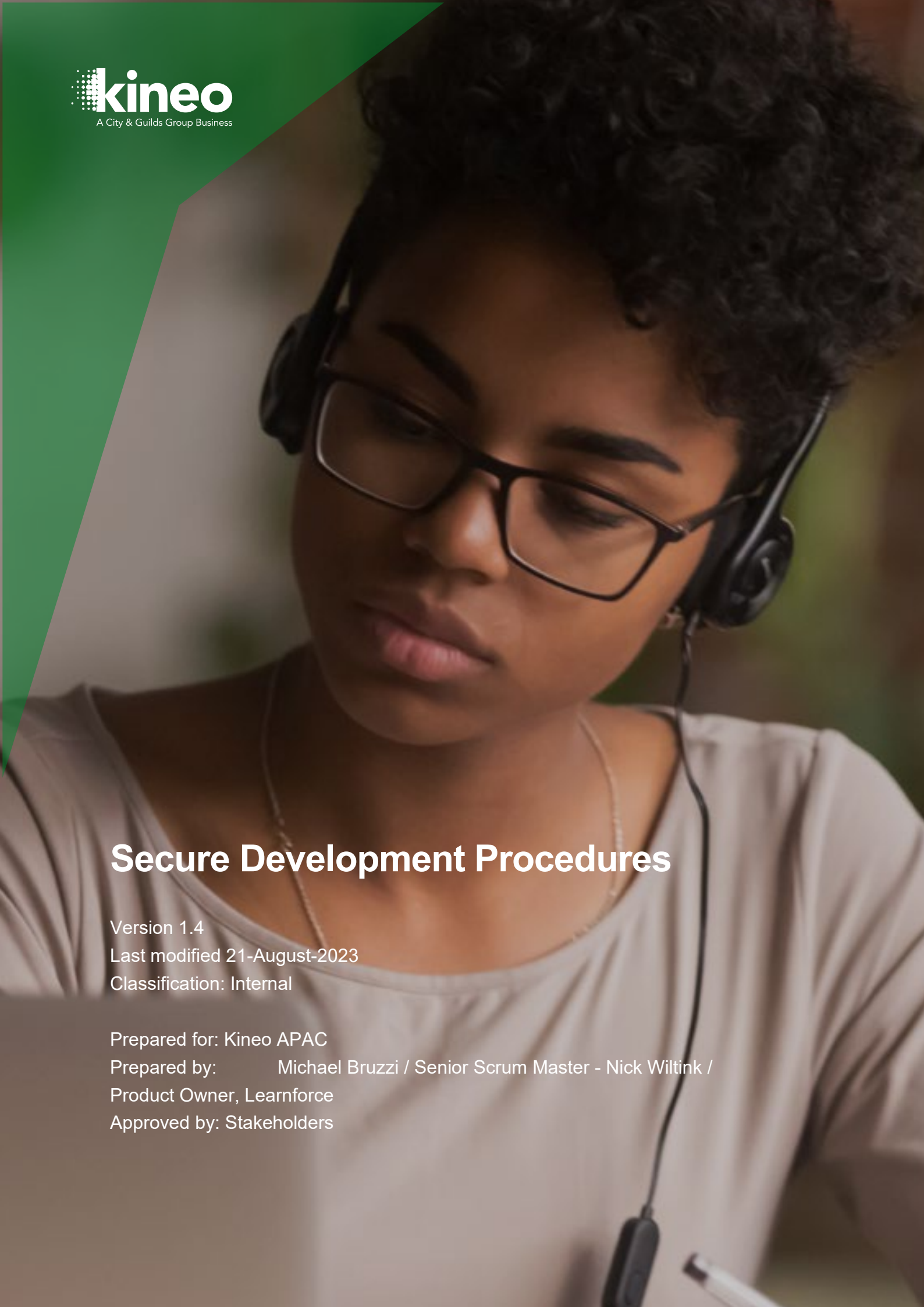


Secure Development Procedures

Version 1.4
Last modified 21-August-2023
Classification: Internal

Prepared for: Kineo APAC
Prepared by: Michael Bruzzi / Senior Scrum Master - Nick Wiltink / Product Owner, Learnforce
Approved by: Stakeholders

Document revision history

Version	Changed by	Summary of change	Approval date
1.0	CQR	Initial Release	1/9/2016
1.1	Jeremy Ninnes	Added Confluence Links	4/11/2016
1.2	Mary Tirado	Change Assessment Team for Release Coordinator	30/06/2017
1.3	Ainsley Renouf	Updated to new Kineo template.	27/03/2018
1.4	Jeremy Ninnes and Russell Grocott	Update and integration of Enterprise Platform	2/07/2019 QSSC 9/07/2019
1.4	Jeremy Ninnes and Michael Bruzzi	No changes done, healthy Check	12/07/2021
1.4	Nick Wiltink and Michael Bruzzi	No changes done, healthy Check	21/08/2023

Contents

1. Purpose

The purpose of this document is to govern when and how to apply requirements for Secure Development Procedures to new applications or changes to existing applications.

These procedures should be read in conjunction with:

- Information Security Management Standard ISO/IEC 27001:2013; and
- Kineo's suite of supporting information security policies.

2. Scope

The requirements and expectations outlined in these procedures apply equally to:

- All fulltime, part time, temporary or casual Kineo employees;
- All contractors engaged by Kineo; and
- All suppliers providing services to Kineo.

It encompasses all Kineo information assets (or resources) which comprise information in all forms, software and hardware.

3. Roles & Responsibilities

Step	Additional Information and Resources
Senior Leadership Team	The provision and implementation of assets, supporting systems, applications, and processes that give effect to these procedures. The establishment and maintenance of monitoring and compliance systems and processes to ensure that the supporting mechanisms are functioning effectively.
Managers and supervisors	The proper induction of new users, including non-permanent personnel, and to ensure that all users in their area are made aware of these procedures and their method of use.
Employees, contractors, and suppliers	Responsibly for compliance with these procedures and supporting policies, standards, and procedures.
All personnel	Reporting security incidents and any identified weaknesses.

4. Principles

4.1. Internal & Externally Developed Applications

Internally and externally developed applications are treated significantly differently. At a high level:

- The process for internal development defines how to create resilient applications;
- Whereas the process for externally developed applications describes how to ensure quality requirements are appropriately communicated to the vendor and tested as part of acceptance.

4.2. Responsible party

- This document identifies the person who is responsible for ensuring that the defined process steps are completed. In most cases, this person will not undertake the activity themselves, but acts in an oversight and governance position.
- The responsible party is accountable if a process step is not followed.

4.3. Known vulnerabilities

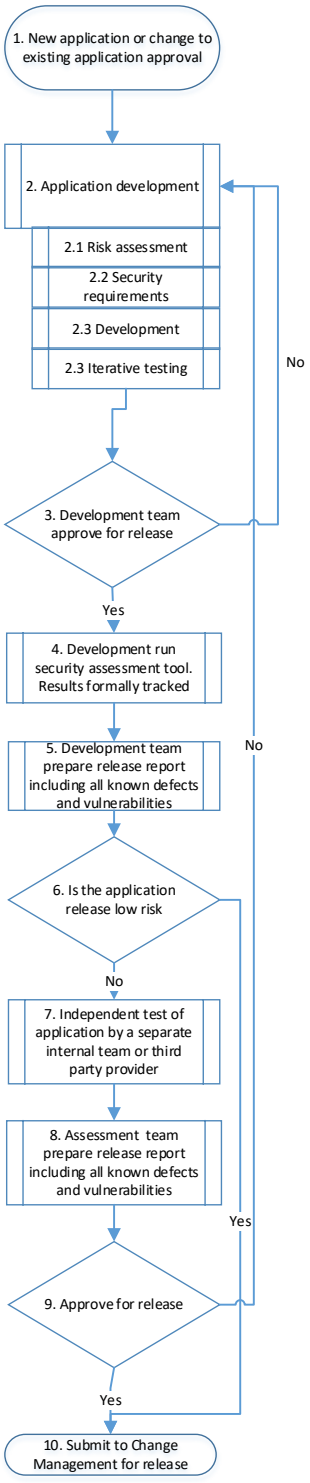
- For a variety of business reasons, it may be appropriate to release an application with known vulnerabilities.
- It is critical that vulnerabilities are accurately recorded to allow the business to make an informed risk/reward decision as to whether an application is ready for release.

4.4. False positives

- Vulnerabilities assessed as false positives are to be included in reports, including a statement on why they were assessed as a false positive.

5. Internal application development

5.1. Process Flow



Further detail for each stage is presented on the next page.

Figure 1 – Internal Secure Application Development Flow

5.2. Process Description

Process ID	Name	Description	Applicable Procedure	Responsible Party
1	New application or change to existing application approved	The standard organisational process for approving the creation or modification of an application and allocation of resources.		Application owner
2	Application development	Application development lifecycle.		
2.1	Risk assessment	Analyse the risk the application presents to the business.	1. Risk assessment	Project manager (or application owner if no project manager)
2.2	Security requirements	Define the security capability requirements of the applications.	2. Security requirements in design phase	Project manager (or application owner if no project manager)
2.3	Development	Write the application code.	5. Secure development environment	Development team leader
2.4	Iterative testing	Test the application using a combination of tools including the secure code assessment tool. Issues may or may not be tracked as formal defects at the discretion of the team leader.	6. Software development. 7. System security testing	Development team leader
3	Development team approve for release	Team leader reviews suitability of application for release including security test results. Applications should only be passed when te team leader is confident the application is ready for production release.		Project manager (or application owner if no project manager)
4	Development team run security assessment tools and formally tracks all results	The development team runs final pass of the security assessment tool and formally tracks any defects or vulnerabilities.	7. System security testing	Development team leader
5	Development team prepare release report	The development team prepares a release report including all known defects and vulnerabilities. The development team is to include the rationale for release with listen known defects or vulnerabilities.		Development team leader
6	Is the application release low risk	The application owner (with advice as required) assesses the risk of the application release.		Project manager (or application owner if no project manager)

		Low risk releases are submitted to the Change Approval Board (CAB) for release. Other releases are subjected to independent testing.		
7	Independent test of the application	An internal or external team not involved in the development of the application undertakes testing of the application using the assessment tools.	7. System security testing	Project manager (or application owner if no project manager)
8	Release Team prepares a release report	Identified vulnerabilities are verified and assessed for impact. This information is included in a report for business owner.		Release coordinator
9	Release approval	Any outstanding risks are assessed, and a business decision is made on whether the application is ready for release. The decision is made by the application owner.		Project manager (or application owner if no project manager)
10	Submit via Release Manager for release	The Release Manager process manages implementation.	10. Implementation	Project manager (or application owner if no project manager)

Note that "application" refers to both the development of a new application and a change to an existing application.

6. External Application Development

6.1. Process Flow

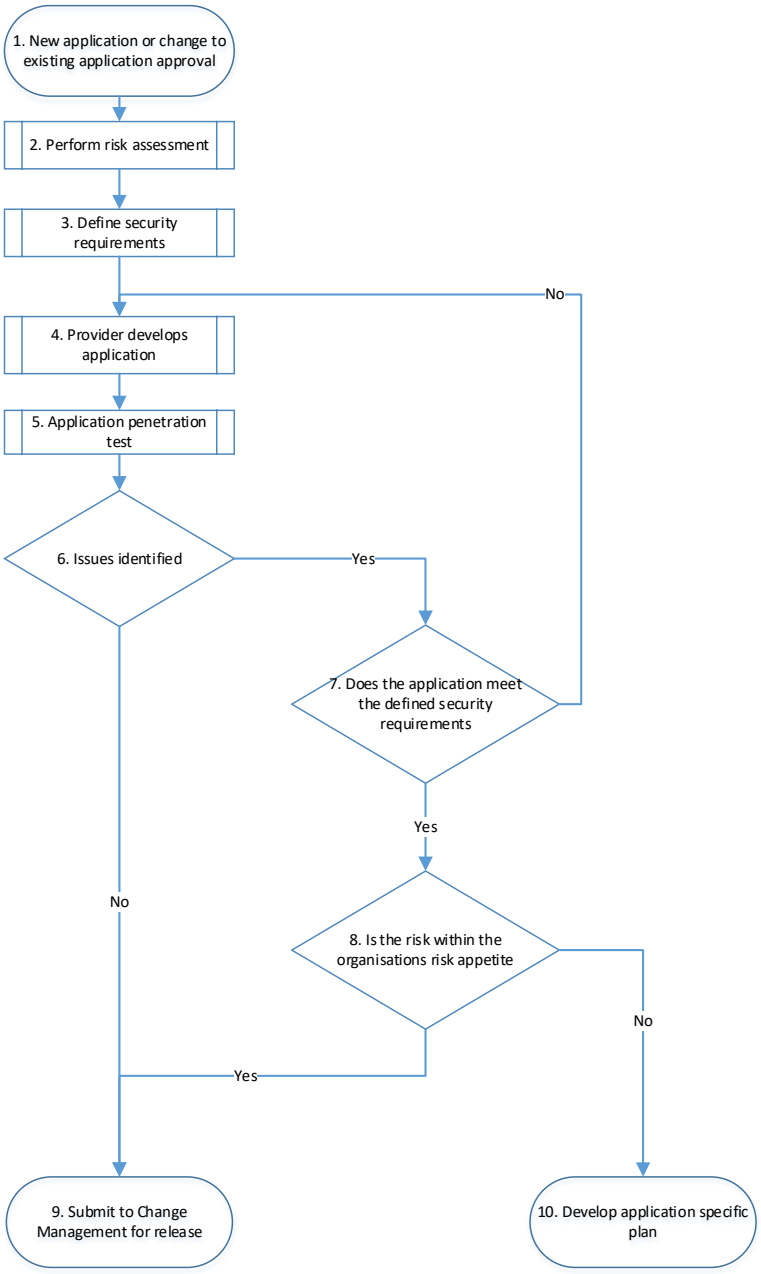


Figure 2 - Internal Secure Application Development Flow

6.2. Process description

Process ID	Name	Description	Applicable Procedure	Responsible Party
1	New application or change to existing application approved.	The standard organizational process for approving the creation or modification of an application and allocation of resources.		Project manager (or application owner is no project manager)
2	Perform risk assessment	Analyse the risk the application presents to the business.		Project manager (or application owner is no project manager)
3	Define security requirements	Define security capability requirements as part of the quality acceptance criteria. The resilience of the application against targeted attack will generally fall within the following three definitions: Level 1 – Not sscptible to semi-skilled attack by individuals using automated tools. Level 2 – not susceptible to skilled attack by individuals using automated tools and targeted exploitation. Level 3 – Not susceptible to highly skilled attack by a team using bespoke tools and techniques. Planning of security testing.	2. Security requirements in design phase. 3. Acquisition. 4. Outsourced Development. 7. System security testing.	Project manager (or application owner is no project manager)
4	Provider develops application	Team leader reviews suitability of application for release including security test results. Applications should only be passed when the team leader is confident the application is ready for production release.		Project manager (or application owner is no project manager)
5	System acceptance testing	Run test plans created in step 3. A penetration test is undertaken in line with the level defined in step 3.	8. System acceptance testing	Project manager (or application owner is no project manager)
5.1	Testing data	Sanitisation of testing data to ensure no sensitive information is compromised.	9. Protection of test data	Tester
6	Issues identified	Are any vulnerabilities identified in testing? If no issues are identified, then the		Project manager (or application owner is no project manager)

		application can be passd to the CAB for release. Otherwise the application needs to be assessed to see if it meets the quality assessment criteria.		
7	Does the application meet the defined security requirements?	Does the application meet the requirements defined in step 3? If not, then acceptance of the application is rejected from the vendor. If the vulnerabilities are within the defined quality criteria, go to step 8.		Project manager (or application owner is no project manager)
8	Is the risk within the organisation's risk appetite?	Any outstanding risks are assessed, and a business decision is made on whether the application is ready for release. This decision is made by the application owner. If the risk is not acceptable, an application specific resolution plan needs to be developed. If the risk is acceptable, then the application is submitted to the CAB for release.		Project manager (or application owner is no project manager)
9	Submit to Change Management for release	The change management process manages implementation.	10. Implementation	Project manager (or application owner is no project manager)
10	Application specific plan	In the event that the application has met the security requirements as defined to the vendor but presents an unacceptable risk to the organization, a situation specific plan needs to be developed on how this is to be managed.		Project manager (or application owner is no project manager)

7. Procedures

7.1. Risk Assessment

A thorough understanding of the business requirements and need to protect confidentiality, integrity and availability of the data to be processed is essential if systems are to fulfil their intended purpose.
This is achieved through:

- Understanding system requirements considering:
  - Capacity;
  - Continuity;
  - Flexibility (i.e. ability to support future changes);
  - Connectivity (e.g. interfaces to existing systems, networks or external resources);
  - Compatibility (e.g. with particular technical environments or components).
- Conducting a threat assessment;
- Identifying vulnerabilities;
- Documenting known risks; and
- Selecting appropriate security controls.

Kineo shall ensure that:

- Project level risks are identified and evaluated based on the desired functionality of the software being developed;
- Risk assessments follow Kineo's risk management methodology;
- The risk ranking assigned to vulnerabilities includes the identification of "high risk" and "critical" vulnerabilities; and
- Risk assessments consider legal and regulatory requirements, such as compliance to the Payment Card Industry Data Security Standard (PCI DSS) or the Privacy Act (1988).

7.2. Security Requirements in Design Phase

Kineo documents design requirements in Confluence using the User Story Template. This template calls out Technical, Security, Design, Usability and Testing requirements for software design.
Kineo shall ensure:

- Information security requirements and associated processes are integrated in the early stages of projects through early engagement with information security personnel;
- Information security requirements and controls reflect the business value of the information involved and the potential negative business impact which might result from lack of adequate security;
- Security requirements are necessary, unambiguous, consistent, complete, concise, feasible, traceable and verifiable;
- Vague security requirements are avoided;
- Assessments consider:
  - The level of confidence required toward the claimed identity of users;

    - Access provisioning and authorisation processes, for business users as well as privileged users;
    - The required protection needs of the assets involved, considering availability, integrity and availability;
    - Business needs around monitoring, such as transaction logging, monitoring or non-repudiation requirements;
    - Mandated security requirements of other systems.
- Information security requirements are documented and reviewed by all stakeholders;
- Security checkpoints are carried out at key project milestones;
- Baseline security requirements for new information systems and enhancements to existing information systems are documented;
- Projects are audited as defined by the security plan to ensure security requirements are evaluated and implemented.

7.3. Acquisition

If products are acquired, a formal testing and acquisition process must be followed by Kineo to ensure that the required functionality does not compromise the security of systems.
To support this requirement Kineo shall document procedures for acquiring software that enable system owners to:

- Describe a concept or need to acquire, develop or enhance a system, software product or software service;
- Analyse system requirements;
- Conduct an initial risk assessment of the proposed product;
- Identify security functionality requirements.

On approval of the concept, Kineo shall:

- Document a security plan detailing the required security controls;
- Obtain assurance that the system is adequately secure;
- Review the level of service and quality offered by the vendor;
- Document a service level agreement (SLA) that includes elements such as:
    - Identification of application owner;
    - Who will provide the service (internal or external);
    - Capacity requirements;
    - Maximum tolerable down time;
    - Criteria for measuring the level of service;
    - Reporting requirements;
    - Critical timescales.
- Ensure that future support for the software product is planned;
- Ensure that the required documentation is available;
- Document the security controls the system must contain;
- Obtain approval for detailed proposals before work commences;
- Document a security test and evaluation plan, detailing how the security controls are to be evaluated before the system is approved and deployed.

Where the security functionality of the proposed product does not satisfy the specified requirements, the risk introduced, and associated controls should be reconsidered prior to purchasing the product.

7.4. Outsourced Development

When software development is outsourced the following must be considered:

- Licensing arrangements regarding code ownership and intellectual property rights associated to the outsourced content;
- Contractual requirements for secure design, coding and test practices;
- Acceptance testing for quality and accuracy of deliverables;
- Provision of evidence that security thresholds were used to establish minimum acceptable levels of security and privacy quality;
- Provision of evidence that sufficient testing has been applied to guard against the absence of both intentional and unintentional malicious content upon delivery;
- Provision of evidence that sufficient testing has been applied to guard against the presence of known vulnerabilities;
- Escrow arrangements, e.g. if source code is no longer available;
- Contractual right to audit development processes and controls; and
- Effective documentation of the build environment used to create deliverables.

When software development uses Open Source components the following must be considered:

- Licensing arrangements regarding use of the component in a commercial environment;
- Licensing agreements regarding requirements for release and/or publication of modifications to source code;
- Active development status of the component;
- History of detection and correction of security defects in the component.

7.5. Secure Development Environment

To ensure a secure environment for system development activities and avoid disruption to business activities, projects are to establish secure development environments which are isolated from the live and testing environments and protected from unauthorised access. Assets within the development environment must be protected against unauthorised access. Therefore, when designing the environment, Kineo should consider:

- The sensitivity of the data to be processed, stored and transmitted by the system;
- Applicable external and internal requirements, e.g. from regulations or policies;
- Security controls already implemented within Kineo that support system development;
- Trustworthiness of the personnel working within the environment;
- The degree of outsourcing associated with system development;
- The need for segregation between different development environments;
- Control of access to the development environment;
- Monitoring change to the environment and code stored therein;

- The separation of duties between personnel assigned to the development/test environments and those assigned to the production environment;
- Back up arrangements; and
- Control of movement of data from and to the environment.

Secure development procedures are required to ensure that processes support the security requirements and that the level of protection is communicated and understood by all relevant personnel.

7.6. Software Development

Secure programming techniques should be used for both new developments and in code re-use scenarios, where the standards applied to development may not be known or were not consistent with current best practices.
Kineo shall ensure:

- System build procedures are documented (see Release Procedures);
- Testing and code reviews verify the implementation of secure code;
- Staff comply with good practice for system coding
- All developers are aware of and follow the Learning Portal coding guidelines
- Insecure design techniques are prohibited (e.g. hard coded passwords, unapproved code samples, web-enabled tools and database products);
- Source code is protected from unauthorised access and tampering;
- Automated tools are used to ensure adherence to coding standards (see Sonar); and
- Code review results are reviewed and approved by management prior to release.

Where access to third party source code is not granted, a copy should be maintained in escrow by a trusted third party until fulfilment of the contract or SLA and checked regularly to ensure it is up to date.

7.7. System Security Testing

New and updated systems require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions.
Kineo shall ensure:

- Documented procedures define the process for testing a system under development covering:
  - The types of software and services to be tested;
  - The use of test plans, including user involvement;
  - Key components of the testing process such as testing of functionality, use under normal and exceptional conditions, the impact of bad data and the effectiveness of security controls;
  - Fall back processes;
  - Process for sign-off of the testing process.
- Initial tests are performed by the development team;

- Quality assurance is undertaken to ensure that key security activities are carried out during the system development life cycle;
- Independent acceptance testing is carried out to ensure that the system works as expected and only as expected;
- The extent of the testing is in proportion to the importance and nature of the system.

7.8. System Acceptance Testing

Systems under development are to be subject to rigorous acceptance testing in a separate area that simulates the production environment.
System accepting testing must include:

- The running of the full suite of system components;
- Full integration testing, to ensure no adverse effects on existing systems;
- The testing of information security requirements as specified within the security plan;
- Attempts to compromise the security of the system (e.g. penetration testing);
- The use of tools to verify the remediation of security related defects;
- Adherence to secure system development practices.

7.9. Protection of Test Data

The use of operational data containing personally identifiable data or any other confidential information for testing purposes should be avoided. For example, live Primary Account Numbers (PANs) are not to be used for testing or development.
If personally identifiable or otherwise confidential data is used:

- All sensitive details and content should be protected by removal or modification;
- Access control procedures, which apply to operational systems, must also apply to the test system;
- Authorisation for its use must be obtained each time operational data is copied to a test environment;
- The copying and use of operational data should be logged to provide an audit trail.

7.10. Implementation

The following checks must be performed before a new system is promoted into the live environment:

- Assurance that security assessments have been carried out;
- Limitations of security controls have been documented;
- Performance and capacity requirements can be met;
- All necessary patches and updates have been tested and successfully applied;
- All development problems have been reviewed and treated or accepted based on risk assessment;
- Assurance has been provided that there will be no adverse effects on existing live systems;
- Any accepted risks are formally documented and accepted by the Information Security Management Forum;
- Details of accepted risks are recorded to prevent them being raised again in production;

- Arrangements for fall-back have been established together with relevant operating procedures;
- Approval has been obtained from an appropriate business representative;
- All development, test and/or custom application accounts, user IDs and passwords are removed before applications become active or are released;
- Test data (including business information) will not be promoted

7.11. Managing Exemptions to Policy Requirements

In circumstances where changes cannot be carried out in compliance with the System Acquisition and Development Policy, formal approval for the changes must be made by System developer and risks accepted by the application owner.

Where certain actions required in the policy are likely to impact the delivery expectations of the business, The ISMS Owner is authorised to approve exemptions to the required policy. The Information Security Management Forum must assess the impact of the operational systems if secure development activities are not carried out.

Where possible, consider retrospectively completing some of the required tasks to ensure that the business gets what it needs, and IT is able to maintain a secure environment.

7.12. Audit

Systems development activities are to be audited by an independent party to ensure that security controls are designed effectively, and risks are managed.

- Audits should cover:
- Roles and responsibilities
- Development methodology and environments
- Local security management
- Adherence to business requirements (for function, security and performance)
- Design and build processes
- Testing processes
- Acceptance testing
- Post implementation review

Discover how we're shaping the future of learning

Everything we do at Kineo stems from a simple idea – if we design a better learning experience, together we'll get better results.

Kineo helps the world's leading businesses improve performance through learning and technology. We're proud of our reputation for being flexible and innovative, and of our award-winning work with clients across the world

Whatever your business challenge, we will partner with you every step of the way to find the learning solution that fits best – and delivers results.

So, how can we help you?
Get in touch about your digital learning challenges

Kineo UK
info@kineo.com
+44 (0)1 273 764 070

Kineo USA
usinfo@kineo.com
+1-312-846-6656

Kineo APAC
info@kineo.com
+61 1300 303 318

www.kineo.com

kineo
A City & Guilds Group Business