INFORMATION SECURITY MANAGEMENT SYSTEM

EXTERNAL INFORMATION SECURITY POLICY

Version:	0.1
Date of version:	24/05/2021
Created by:	S.Giachardi J. Baskerville
Approved by:	C. Franks
Confidentiality level:	PUBLIC

Change history

Date	Version	Created by	Description of change
24/05/2021	0.1	S. Giachardi	Initial Draft
24/05/2021	1.0	J. Baskerville	Approved Version

Table of Contents

1 Purpose, Scope and Users

The aim of this Policy is to define the purpose, direction, principles and basic rules for Information Security Management within Qubeeo Ltd trading as StoryStream.

This policy is intended to ensure that StoryStream information can be used when required with the confidence that it is accurate and complete, and that it is adequately protected from misuse, unauthorized disclosure, damage or loss. The policy reinforces the value of data and information to StoryStream.

This External IT Security Policy sets out management's information security direction and is part of the StoryStream Information Security Management System (ISMS). The purpose of the ISMS is to proactively and actively identify, mitigate, monitor and manage information security vulnerabilities, threats and risks in order to protect StoryStream and its assets, information and data.

The ISMS sets the intent and establishes the direction and principles for the protection of StoryStream's IT assets. This is to enable continuous improvement of StoryStream security capability and resilience to emerging and evolving security threats.

This Policy is representative of the controls applied to the entire Information Security Management System (ISMS), as defined in the ISMS Scope Document.

This policy is intended for public use by external users, third parties and other interested parties.

2 Basic Information Security Terminology

Confidentiality – Characteristic of the information by which it is available only to authorised persons or systems.

Integrity – Characteristic of the information by which it is changed only by authorised persons or systems in an allowed way.
Availability – Characteristic of the information by which it can be accessed by authorised persons when it is needed.
Information security – Preservation of confidentiality, integrity and availability of information.
Information Security Management System – Part of overall management processes that takes care of planning, implementing, maintaining, reviewing and improving information security.

StoryStream values the use of information technology in supporting the mission of the organization and its clients. StoryStream information, managed and residing on StoryStream resources is an important asset that must be protected. Any person or organization that uses these assets has a responsibility to maintain and safeguard them.

StoryStream is committed to preserving the confidentiality, integrity, and availability of information regardless of the form it takes - electronic or non-electronic.

Improper use of information resources may result in harm to StoryStream and its mission.

3 Managing the Information Security

3.1 Objectives

General objectives for the Information Security Management System (ISMS) are the following:

- To ensure the security of information shared with StoryStream.
- To reduce the potential / opportunity for security incidents to harm information shared with StoryStream.
- To ensure that only authorised individuals can access information shared with StoryStream.
  To preserve the integrity of information shared with StoryStream.
- Goals are in line with the organization's business objectives, strategy and business plans.

CEO is responsible for reviewing these general ISMS objectives and setting new ones.

CTO is responsible for ensuring these objectives are met.

Objectives for individual security controls or groups of controls are proposed by:

- Data Protection Officer
- Chief Technical Officer
- Chief Operating Officer

and approved by:

Chief Executive Officer in the Statement of Applicability.

StoryStream supports an extensively broad and complex data landscape. Based on appropriate data classification and handling guidelines, this policy and associated standard ensures that appropriate controls are implemented for the confidentiality and integrity of sensitive data.

3.2 Measurement

StoryStream measures the fulfilment of its security objectives using internal metrics and key performance indicators. StoryStream reviews its security objectives annually to ensure that the business is meeting its security objectives.

The DPO is responsible for setting the method for measuring the achievement of the objectives – the measurement will be performed at least once a year and the DPO will analyse and evaluate the measurement results and report them to the management team as input materials for the management review.

4 Policy Statement

StoryStream ensures that all necessary management direction and support for Information Security is provided with the agreement and support of the Information Security Committee and the Board of Directors.
Reviews of all the Information Security Management System policies and associated documents shall be performed regularly, at least once per year, or when significant change occurs within the business.

4.1 Organisation of Information Security

4.1.1 Policies for Information Security

- A set of information security policies has been defined and approved by the senior management team. StoryStream's Information Security policies are published on an easily accessible location and communicated to all employees including contractors and relevant external third parties as required.

4.1.2 Information Security Roles and Responsibilities

- Responsibilities for information security are listed in various ISMS documents. If required, Head of IT defines additional responsibilities .
- Conflicting duties and areas of responsibilities shall be segregated to reduce opportunities for authorisation or unintentional modification or misuse.

4.1.3 Information Security in Project Management

- Information security shall be addressed in project management regardless of the type of project.

4.1.4 Risk Management

- A Risk Management Framework shall exist which provides an approach to the identification, classification and treatment of information risks.

4.2 Human Resource Security

4.2.1 Prior to Employment

- Where legally permissible, all employees shall be screened prior to employment to ensure suitability for their role.
- The contractual agreements with employees and contractors shall state their and StoryStream, responsibility for information security.

4.2.2 During Employment

- Continuous training around information security awareness shall be given to new and existing employees annually or when there is a significant change. Key staff may receive specific sessions if required.
- When a member of staff leaves, no matter what the circumstance, a thorough leaver process shall be followed to prevent accidental or deliberate account misuse.
- StoryStream shall have a documented and communicated disciplinary process to act against employees and contractors who have committed an information security breach.

4.3 Asset Management

4.3.1 Inventory of Assets

- All assets, tangible and intangible, shall be identified, managed and maintained to ensure control.

4.3.2 Information Classification

- Information shall be classified in terms of legal requirements, value, criticality, and sensitivity to unauthorised disclosure or modification

4.3.3 Media Handling

- StoryStream has banned the use of removable media within the organisation.

4.4 Access Control

4.4.1 Management of Privileged Access Rights

- StoryStream shall document a formal Privileged Access authorisation process
- Privileged access rights shall not be granted until the authorisation process is complete.
- Privileged access rights shall be allocated to employees, third parties and sub-contractors, on a need-to-use, on an event-by-event least privilege basis
- Privilege access shall be assigned to a user ID different from the one used for regular business activities. Regular business activities shall not be performed using a privileged ID.
- Records of all privileges allocated shall be maintained and reviewed by StoryStream CTO and the employee's line manager on a regular basis or quarterly at a minimum, in order to verify usage and access is in line with the employee's roles and responsibilities and shall be revoked if necessary.
- StoryStream shall set the requirements for expiry of privileged access rights. The duration shall be determined by the information system owner.

4.4.2 Access to Networks and Network Services

- Access to networks and network services shall only be provided to properly authenticated authorised users.

4.4.3 Joiners, Movers and Leavers Process

- A formal user registration and de-registration process shall be implemented to enable assignment of access rights, this process shall be in line with HR procedures and processes.

4.4.4 Password Management

- Access to confidential information processing systems and applications shall only be granted following successful user authentication in line with StoryStreams password management procedures.

- Unique credentials shall be given to each employee in order to enforce non-repudiation and to allow for audit and tracking for accountability and monitoring purposes.

4.5 Cryptography

4.5.1 Encryption

- External data in transit shall be encrypted to a minimum of TLS1.2, HTTPS.
- The use of APIs within StoryStream shall be accessed over HTTPS, in conjunction with proprietary authentication and authorisation mechanism, such as the use of tokens.

4.6 Physical Security

4.6.1 Physical Entry Points

- Unauthorised physical access and interference shall be prevented by multiple layers of security, such as but not limited to;
  - CCTV shall cover the entry point into StoryStream's office
  - Access into StoryStream offices and sites during and out of business hours shall be monitored and regularly reviewed.

4.6.2 Equipment

- StoryStream shall ensure all equipment shall be securely protected and located to prevent loss, damage, theft, compromise or interruption to StoryStream's operations.
- Classified assets shall be protected from unauthorised access and use.
- All screens and desks shall be clear of confidential assets whilst unattended.

4.7 Operational Security

4.7.1 Change Management

- Changes to StoryStream systems (live, test and development) shall be controlled through a change management process ensuring all changes are agreed, authorised, documented and reviewed.

4.7.2 Protection from Malware

- Detection, prevention and recovery controls shall be implemented on all devices used whilst accessing and processing data to protect against malware.
- Controls shall be implemented to protect all incoming emails and other forms of communication from malicious threats.

4.7.3 Logging and Monitoring

- Event logs shall be recorded, monitored and reviewed on a regular basis to identify unauthorised access and activity.
- Logs shall be protected from unauthorised access or modification.

4.7.4 Vulnerability Management

- Technical controls shall be implemented to identify and remediate vulnerabilities in a timely fashion.
- StoryStream shall ensure there are technical controls implemented to identify malicious external activity
- Vulnerabilities shall be scanned on a regular basis with tailored alerts sent to StoryStream CTO for review.

4.8 Communications Security

4.8.1 Network Security

- Network security controls shall be implemented to manage and control StoryStream's applications and systems.

4.9 System Development and Maintenance

4.9.1 Security in Development

- Requirements for security controls shall be addressed prior to any new system or existing system enhancement.
- User access to software, test data and source code shall be restricted and monitored. Industry class software shall be deployed to control external ports on laptops to help prevent data leakage.
- Authorisation must be sought from StoryStream CTO prior to the sharing of any internal network details which can but not limited to include diagrams, routing information, IP addresses etc. The sharing of this information is strictly prohibited unless the prior correct authorisation has been gained.

4.9.2 Test Data

- Live data shall not be used in a test or pre-production environment.
- Data shall be anonymised and obfuscated before being used in a test or pre-production environment.

4.10 Supplier Relationships

4.10.1 Management of Third-Party Suppliers

- StoryStream shall ensure all third-party suppliers' responsibility for information security is defined and documented.

4.11 Information Security Incident Management

4.11.1 Management of Information Security Incidents

- Security Incident Management processes shall be aligned with ISO 27001:2013, ISO 27035:2016, and NIST SP 800-61.
- All staff shall receive guidance on reporting such incidents.

4.12 Business Continuity Management

4.12.1 Information Security Continuity

- Clear and comprehensive Business Continuity Plan (BCMP) is in place, to counteract the interruption to business activities and the ability to deliver services.
- BCP requirements shall be tested annually with a review of the plans every six months.

4.13 Compliance

4.13.1 Compliance with Legal and Contractual Requirements

- StoryStream shall comply with all relevant regulatory, legal and contractual requirements to avoid any breaches.
- StoryStream shall ensure appropriate procedures are in place to ensure the confidentiality, integrity and availability of personally identifiable information in line with the principles set by the EU General Data Protection Regulation (EU GDPR) and the UK Data Protection Act (DPA) 2018.

4.14 Responsibilities

Responsibilities for the ISMS are the following:

- DPO is responsible for ensuring that the ISMS is implemented and maintained according to this Policy
- CEO is responsible for ensuring all necessary resources are available
- CTO is responsible for operational coordination of the ISMS as well as for reporting about the performance of the ISMS
- ISO Management Team must review the ISMS at least once a year or each time a significant change occurs and prepare minutes from that meeting. The purpose of the management review is to establish the suitability, adequacy and effectiveness of the ISMS
- DPO will implement information security training and awareness programs for employees
- The protection of integrity, availability, and confidentiality of assets is the responsibility of the owner of each asset
- All security incidents or weaknesses must be reported to the CTO and COO
- DPO will define which information related to information security will be communicated to which interested party (both internal and external), by whom and when
- DPO is responsible for adopting and implementing the Training and Awareness Plan, which applies to all persons who have a role in information security management

4.15 Policy Communication

The DPO has to ensure that all employees of StoryStream, as well as appropriate external parties, are familiar with this Policy.

5 Support for ISMS Implementation

Hereby the CEO declares that ISMS implementation and continual improvement will be supported with adequate resources in order to achieve all objectives set in this Policy, as well as satisfy all identified requirements.

6 Validity and Document Management

This document is valid as of 24 May 2021.

The owner of this document is CEO, Alex Vaidya, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Number of employees and external parties who have a role in the ISMS, but are not familiar with this document
- Non-compliance of the ISMS with the laws and regulations, contractual obligations, and other internal documents of the organisation
- Ineffectiveness of ISMS implementation and maintenance
- Unclear responsibilities for ISMS implementation

Data Protection Officer

Cameron Franks

_____

[signature]