INFORMATION SECURITY AND BUSINESS CONTINUITY POLICY

Purpose

To ensure business continuity and minimise business damageURIMegrity and availability of the Company's operations, services and information.

Scope

The provision of Global Content Management Services by URIM App Limited ("URIM").

Policy

URIM's strategy is to ensure the right framework is in place to identify and mitigate the risks to an acceptable level, in order to protect our stakeholders, systems and infrastructure.

Information is vital to the efficient and effective operation of URIM. As such, information will only be used for its intended purpose, i.e. in support of URIM operations. Similarly, Client Data will only be used in support of the delivery of Services in accordance with the associated Client Service Contracts.

To protect the Company's operations and information assets[1] from all threats, whether internal or external, deliberate or accidental, and thereby seek to maintain **100%** availability of Contractual Content Management Services delivered to clients.

Operation and Information assets include:

- Personal Information about employees & other stakeholders, within URIM, its customers and suppliers.
- Corporate information including strategies, financial and contractual performance.
- Technical and functional product and service information.
- Contractual and corporate information about our customers
- Contractual information about business consultants, business partners, stakeholders and third party suppliers.
- Legal, regulatory and statutory information.
- Technical hardware, equipment and software systems
- Physical buildings and offices
- Employees, contractors and third parties

The information security and business continuity requirements will continue to be aligned with the Company's goals and objectives.

To take all reasonable steps to ensure that in the event of a disruption URIM can continue to deliver an acceptable level of service of its key activities, URIM ensures that:

- Information will be protected against **unauthorised access.**
- **Confidentiality** of information will be assured.
- **Integrity** of information will be maintained.
- **Regulatory** and **legislative** requirements will be met.

[1] Information takes many forms and includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes and diskettes, or spoken in conversation and over the telephone

- The **continuity** of key services and the supporting critical activities will be assured
- **Information security and business continuity training** will be available to all staff.

All major operational incidents and breaches of information security, actual or suspected, will be reported to and investigated by the Chief Executive Officer (CEO), who is also URIM's DPO & CISO.

Business Management System

The Business Management System (BMS) defines the ***framework*** for the development and application of URIM's activities undertaken to meet the evolving requirements of the Company's overall Information Security and Business Continuity Policy.

This Policy applies to all activities undertaken by URIM, irrespective of whether its own, or third party/subcontracted resources are used. The Policy is issued under the authority of the CEO of URIM.

Objectives

The objectives of this Information Security and Business Continuity Policy are to:

- Reduce operational and information security risks to an acceptable level (Low).
- Establish the necessary policies and processes and organisational structure that will protect the Company's assets and key activities from all appropriate threats, so aligning with emerging business strategy & underpinning stakeholder value, whilst ensuring relevant risks to assets are being appropriately addressed.
- Ensure that URIM assets are appropriately protected and yet remain available in line with business requirements & relevant prevailing laws and regulations in the jurisdictions in which it operates it Services.
- Ensure that all URIM information, shared with other parties is protected against unauthorised disclosure and is managed in compliance with this Policy.
- Ensure that all management and employees are aware of and comply with applicable legislative and regulatory requirements.
- Maintain staff awareness of information security, thereby ensuring that all employees understand its importance to URIM and their own individual responsibilities for security.
- Ensure that all major operational incidents and breaches of information security, actual or suspected, are reported to and investigated by the CEO who has direct responsibility for maintaining the Policy.
- Ensure that all information controls are implemented to a repeatable and consistently high standard.
- Provide the delivery of controls to agreed requirements, at the right time and at the right cost to the benefit of our customers, shareholders, suppliers and employees.
- Provide documentary evidence in the form of records to show that the processes are being followed correctly and completely.
- Continually improve URIM's BMS, based on customer and staff feedback, incidents, key performance indicator results, audit findings and technologies.

- Enable the rapid dissemination of improvements (effective and / or efficiency) to all relevant areas.

Key Performance Indicators

- URIM will maintain a programme of 3 formal, planned Tests of its prevailing BCP annually (referred to as: Exercises, Rehearsals & Tests, depending on scale)
- The BCP document itself will be audited & reviewed at least twice annually, as part of the established Company Review process
- URIM's entire operations shall be audited annually to ISO 22301 standards
- Any actual or potential breaches of this policy will be escalated to the CEO immediately upon identification & managed through to resolution under the relevant formal Incident Management procedures, supervised under the monthly Operations Review process
- **The above KPIs & objectives will be monitored, evaluated & reviewed as part of the ongoing Operations Review process**

Principles

As a company, URIM prides itself on the delivery of products and services, to its customers, that are safe and secure. Adoption of and adherence to the BMS enables the Company to analyse its information security and business continuity requirements and define processes which will contribute to the provision of a secure and operational service that is acceptable to the customer. The BMS provides the framework for continual improvement and thus potentially enhancing customer satisfaction.

URIM will develop and maintain an effective documented BMS based on the requirements of the standards **ISO 27001 and ISO 22301**, to ensure that URIM has a documented method of control which protects the Company and its customers.

With the ever-increasing changes in technology and legislation, URIM looks to subject matter experts to provide advice and guidance on the implementation of information security and business continuity policies and practices.

Categorisation

All URIM Information managed under this Policy will be managed in accordance with its Information Security Categorisation. There are 3 Categorisations:

1. Public: This is Information widely available in the Public Domain, such as can be found on URIM's own web site. No special provisions as to its access & secrecy need be made. However, reasonable endeavours will be made by URIM so as to maintain its accuracy, integrity & availability, in support of URIM Operations.
2. Private: This is Information that is deemed by URIM (defaulting to the information owner, or creator, supervised by their line management) to carry a low risk of some potential harm to URIM, or its Stakeholders, in the event of it being shared with unauthorised parties. Such information must be protected by appropriate use of Non Disclosure Agreements, Contract clauses regarding secrecy, password protection and physical security measures (eg locked cabinets, or digitally locked screensavers). Where such documentation is shared with third parties, following a suitable risk assessment by the sharer, it must be on a need-to-know basis and clearly marked as "Commercial In Confidence", if not already covered by suitable Contract confidentiality clauses and/or NDA's in place between the relevant parties.

3. Secret: This Information is covered by URIM's highest level of Information Security protection measures. This information carries a high risk of damage or loss to URIM and/or its Stakeholders, if shared with unauthorised parties, or if otherwise not satisfying minimal requirements regarding its confidentiality, access, accuracy, integrity, availability & security. Such Information should be protected by relevant & proportional measures of physical & digital security, which will be managed & reviewed under URIM's maintained Business Impact Analysis Process. Such Information assets include URIM's Intellectual Property, official legal Company Records & Client Personal Data (including but not limited to Personally Identifiable Information), as defined under GDPR and other similar legislation. Details of the extensive proportionate technical measures taken by URIM, in support of protecting Client Personal Data, are provided in the prevailing version of the technical document: "How Does URIM Safeguard My Data?". This sets out the minimum measures undertaken by URIM for all Clients. Additional measures, such as URIM's adherence to core ISF IRAM2 principles, go beyond what is listed and Clients may request details of, or specify such additional measures, sufficient to satisfy their own Operational requirements, on a case-by-case Contractual basis.

Risk Strategy

URIM will follow a risk strategy aimed at balancing the unacceptability of high information risks on one side against unnecessarily expensive and bureaucratic controls on the other.

The implementation of URIM's risk strategy will be based on formal methods for risk assessment, risk management and risk acceptance. By default, URIM has a **LOW** appetite for operational IS & BC risks, given the high reliance of its Clients on the reliability & security of URIM's Contractual notification Services. Its policies, processes & objectives will all serve this overall risk appetite and associated posture. URIM will adhere to core ISF IRAM2 principles, in support of achievement of its Risk Strategy for its Information Assets.

Achievement

To achieve URIM's objectives and demonstrate to clients, potential clients, partners and communications market, our commitment to providing quality products and services the Company maintains a BMS which means that:-

- The information security and business continuity needs and expectations of customers, shareholders and partners will be clearly defined and verified through documentation and reviews.
- Risk assessments will be undertaken to ensure the business requirements for the confidentiality, integrity or availability of information, systems and operational resources will be met.
- A variety of policies, processes, procedures and standards will be created, approved, implemented and reviewed regularly to support this policy.
- Internal audits, External audits, identification and measurements of selected KPIs and management reviews will be conducted to ensure the ongoing effectiveness and efficiency of the Management System.
- Training and development needs will be identified and made available to all employees.[2]

[2] Applies to all employees, contractors, consultants, staff, and independent contractors

- All non-conformances, information security and business continuity incidents will be reported to and investigated by the CEO and suitable action will be taken in a timely manner.
- Where the purchase of products or services has been outsourced to third parties, the management of associated information security and business continuity considerations will be controlled through contracts, definitions of requirements, service level agreements, product / service acceptance and audits, as appropriate.
- Legal, Regulatory and Contractual Compliance – All activities and services provided by URIM will meet Legal, Regulatory and Contractual requirements. These requirements will be documented and the corporate level of compliance assessed. With the support of subject matter experts any new or changed requirements are identified, monitored and actions taken as necessary to ensure ongoing compliance.

Assurance

The BMS will ensure the following:

- Audits – These will be carried out by both internal and external auditors, relevant to the business operations concerned. These audits will be subject to a planned schedule that will cover all the activities against the requirements of the relevant URIM BMS and external standards. All audits will produce a suitably detailed report, identifying any areas of non compliance and specifying the corrective action required. These corrective actions will be the subject of 'close-off' actions by the relevant functional head.
- Performance - The information security and business continuity objectives are formally reviewed. Key performance targets will be identified and subsequently monitored, measured and reported at corporate, programme, and project level as appropriate. The information security and business continuity targets will be regularly monitored for effectiveness and efficiency within the Annual Business Review, six monthly Company Review and monthly operations review. These information security targets will be known by and focused on by URIM staff.
- The business continuity strategy - will be reviewed annually to ensure accuracy of information, and associated strategies. The strategy will be reviewed for possible updating within 45 days of any major operational or system changes which will have a material effect on the contingency strategy.
- Testing - of the business continuity capability will be conducted each year or within 45 days of any major operational or system changes that will have a material effect on the contingency strategy.
- Records - will be maintained throughout the BMS operation as a basis for providing assurance to all associated with, responsible for/or dependent upon the service provided and/or any external accreditation body.

Review

This policy will be reviewed as part of the six monthly Company Review process, or at such time that there has been a significant change to URIM's operations or legal and regulatory requirements.

RESPONSIBILITY AND AUTHORITY

This policy standard for the BMS is issued under the authority of the CEO (& CISO) of URIM. Responsibility for implementation of this policy standard throughout the business is set out below.

- The CEO will be responsible for the overall direction and commitment to information security and business continuity, providing adequate resource, and monitoring / improving its effectiveness. The CEO will have direct responsibility for maintaining the BMS, its associated policies, processes procedures and standards
- All **Functional Managers** will be directly responsible for ensuring that within their business areas all the systems, infrastructure and services provided to the company comply with the relevant policies, processes, procedures and standards as documented within the BMS. As 'owners' they will be responsible for the identification, implementation and maintenance of controls for assets they own and the risks to which they are exposed.
- All **Individuals** will be responsible for ensuring that the tasks they complete, or are responsible for, follow the documented policies, processes, procedures and standards.

Specific responsibilities are described in more detail within the relevant policies and processes.

EVIDENCE OF COMPLIANCE

To demonstrate ongoing compliance with the BMS, the following documentation will be available for audit:

- This Information Security and Business Continuity Policy
- Related policy statements, BC Plan and procedures
- Business continuity strategy
- Business Management System framework
- Process Overview
- Data Protection Policy
- Procedures/work instructions/user requirement documents
- Records

GUIDANCE AND STANDARDS

The following international standards provide useful guidance on the implementation of the best practice information security and business continuity management:

- ISO 27001 Information Security Management Systems – Requirements
- ISO27002 Information Security Management Systems – Code of Practice
- ISO 22301 Business Continuity Management System – Code of Practice
- ISO 22301 Business Continuity Management System - Specification

DOCUMENT CONTROL

Version1	01 April 2019	Initial Version