Data Protection

How Does Urim Safeguard My Data?

bsi. ISO/IEC 27001 Information Security Management

bsi. ISO 22301 Business Continuity Management

bsi. ISO 9001 Quality Management

How Does Urim Safeguard My Data?

Introduction

Any personal data given to URIM by its Clients, is for use within its hosted content management systems only, to deliver the services that it is contractually obligated to provide. Client personal data (such as Contact details, or sensitive company information) is only used by authorized Users of the system itself. Instant messages sent to URIM Users can only be initiated by approved Administrative level Users within the Client's own URIM instance, or exceptionally by URIM support staff, in the normal run of providing support and testing functions. URIM takes seriously its duty of care regarding data, to guard against loss, theft, copying, corruption, or any form of misuse, or abuse.

The purpose of this document is to set out the steps that Urim take to safeguard personal client data entrusted to it as a company.

Information Security Governance Model

Within URIM, responsibility for data is owned by the relevant Department Head for each type of data. The CEO, is the contact point to address any perceived, or potential breaches of URIM's compliance to the company's stated information security policies. Individual staff are responsible for their own data, relevant to their need to access and handle it, respective to their roles. Production system password access is given only to the extent required to perform essential support tasks. Sharing of data internally and externally is governed by European GDPR legislation plus specific NDAs, confidentiality agreements and other contractual arrangements with URIM clients and suppliers. Sharing of client data is on a need-to-know basis, consistent with the relevant contractor, or member of staff, to perform their necessary role. From induction, URIM Staff are trained and instructed to treat all client data in accordance with prevailing data protection legislation and industry good practice. All personal data held within the URIM systems is governed by European GDPR legislation and URIM is governed by the UK's Data Protection Authority (the Information Commissioner's Office).

URIM also actively complies with the EU-US Seven Privacy Shield Principles. This document forms an essential part of that compliance. Any queries, issues, complaints, or other procedural matters relating to URIM's compliance with such legislation, should be directed by email to support@URIMapp.com, where it will be escalated to URIM's CEO for resolution. Independent recourse in such matters is available through the UK's Data Protection Authority. This document is itself made publicly available via the company's web site at www.URIM.app. Over and above the protections provided by these acts, URIM enforces the following security measures to further safeguard customer data.

Physical Security

The services are provided from UK-based, hosted platforms, running within Tier 3 secure hosting sites in in the UK. Hosting sites are managed by specialist data centre operations companies and share the following security features:

- Access to server rooms is restricted with biometric scanning, personal swipe card and PIN protection.
- Premises are controlled by 7x24 security staff on site.
- All key areas, both inside and outside the building, are kept under CCTV surveillance 7x24.
- Delivery, reception, loading and server room areas are all segregated from each other and each has its own access permissions.
- Access to the server rooms from floors above and below is controlled by the same data centre service provider.
- Third parties, such as hardware maintenance engineers, can only access the specific cabinets by prior appointment, with photo ID and accompanied by hosting centre staff.
- Modern Fire detection and suppression equipment and systems are used throughout each data centre.
- Water and leak detection equipment operates to detect any damaging water actions which might harm the data centre equipment.
- As a central strand of its Backup Policy, URIM don't store Client data on any media outside of the data centre (such as off-site tape, CD, or printed off copies).
- No Client data regarding employee contact details is held at URIM administrative offices. Only commercial and account specific information is held at the Administrative offices (eg contracts, NDAs, invoice copies, etc).
- All sensitive physical materials are held in locked cabinets.

Logical Security

- Client access to URIM's hosted notification systems is via a secure Web interface. URIM secures its web interface using Digital Certificates with SSL, for all connections between customer web browsers and the hosted system. As such, all data 'in transit' is encrypted. URIM rotates these certificates on a regular basis.
- URIM's entire hosted infrastructure and associated services are tested annually by specialist, accredited external system security companies, authorised to accredit systems to the UK Government's CHECK certificate level, approved by the UK's CESG. Specialists conduct a range of tests following a detailed method, covering brute force, penetration and vulnerability assessments. Their findings are shared with URIM's CEO. Information regarding their approach and their findings is available for viewing by Clients upon request. In addition, URIM periodically undertake further specialist vulnerability assessments, including SQL injection vulnerability, script hacking and other potential privileged access abuses.
- Firewalls protecting the server environment have IDS (Intrusion DetectionSystem) software installed, preventing unauthorised access to URIM systems.
- Each hosted site is protected by the combination of a firewall and a demilitarised zone (DMZ), to defend against various denial of service and automated web-based attacks.
- URIM's Clients can have services hosted on multiple separate sites, with separate IP addresses, for further protection and resilience.
- Access to the production servers is achieved by support staff, via secure
- VPN connections. Production systems are not connected to any other company networks.
- Corporate server passwords meet the elevated password format standard. URIM's hosted services are periodically reviewed by external auditing bodies, including Client-driven outside service provider (OSP) audits. Details of these can be made available to Clients upon request.
- URIM follow procedures and practices to ISO27001 Security standards, ISO22301 for Business Continuity standards and ISO9001 for its Quality Management System.

Data Security

Data held within URIM hosted systems for each client is held on a unique client database by default. As such, one Client's data is completely logically separated from other Clients. There is no risk of unauthorised transfer between databases.

URIM's Clients upload their own content and data, directly into the URIM system. URIM separates out Development and Test environments from its multiple production systems. No Client data is used on Development systems. Client data on Test systems will be that entered directly by the Client themselves. Test environments are subject to the same physical and logical security measures employed on Production systems.

Staff Checks

Background checks are conducted on all employees, covering criminal background, employer reference and relevant competence checks.

Other URIM Security Procedures and Practices Around Data

1. Access to systems by staff is confined to identified users, whose activity is tracked within the system logs, thereby ensuring personal auditability and accountability.
2. When accessing the system, all staff prove their identity by means of a unique authenticator, which is secret, available only to the individual and never printed, or displayed, ie. password, personal identification number (PIN) or secret code. URIM staff also use individual RSA keys and a unique identifier (a UserID), to distinguish themselves to the computer system.
3. Each person granted access is responsible for ensuring that their unique authenticator is not compromised, and the unique authenticator is changed if they believe this has occurred, advising their security administrator of the circumstances.
4. Staff are able to set up passwords known only to themselves, and are able to alter those passwords when they wish. Passwords have a minimum length of 8 characters and are designed to not be easily guessed.
5. Internal password systems periodically force holders to change their passwords and password systems ensure that when users change their password, they cannot revert to using their old password for at least 5 consecutive password changes.
6. Any passwords entered incorrectly three times in succession are revoked temporarily.
7. Where company laptops in use by staff have the capability of recording a number of keystrokes, including User ID and password entry, and then replaying them on the screen, this facility is disabled.

8. Access to systems is within pre-defined hours. Exceptional access to systems outside of these pre-defined hours, has to be specially authorised by the Head of Operations.
9. Persons do not hold internal system passwords, which would allow them to carry out alone, operations which require dual control, or would grant them a level of authority to which they are not entitled.
10. Access control systems enforce segregation of duties.
11. Where there has been no user activity for a predetermined period of time, internal systems lock the user out and request re-authentication of the user before further activity.
12. Systems detect and deny access by unauthorised personnel or systems, as well as detect misuse of computer facilities, record such attempts, automatically disable such accounts and report them promptly for thorough investigation.
13. Audit trails of unauthorised access attempts are retained for review for a year by URIM Management, together with the results of any investigations undertaken.
14. The URIM Head of Operations, or his deputy, ensures that all requests for the provision of privileged access to computer systems are appropriately authorised by the CEO.
15. Systems have the facility to provide the Security Administrator with sufficient information to enable the administrator, or his deputy, to control and review authorised users and their permitted functions.
16. Audit trails are kept detailing System Administration activities.
17. Where client data is passed on telecommunications links, which extend beyond the physical control of URIM premises, it is protected by encryption.
18. Local Development and Support personnel do not have access to live client confidential data and software, current or historical.
19. Client data is segregated away from other data and any other third party's data, whilst on the Local Servers.
20. Where access to privileged functions, or client data has been granted temporarily to support personnel, to provide emergency support, such access is withdrawn immediately following completion of the support task.
21. Local operators are restricted to those tasks, facilities and utilities, that their normal daily duties require except in exceptional circumstances, e.g. system or software failure. In such circumstances, any variation is logged, usually automatically, and reviewed by management.

22. Utilities and privileged access, which provide the means to make uncontrolled changes to data on the system, are not available to standard system operators.
23. Anti virus tools are installed on all servers and URIM client access systems and are kept regularly updated.
24. URIM use industry recognised System Development Life Cycle models for all new development work.
25. Penetration testing is carried out on the infrastructure and systems by designated specialist outside contractors, authorised to certify to the CESG's CHECK certificate level and above.
26. Updates to the web site are controlled using strong authentication mechanisms e.g. hardware authentication. All changes automatically logged and tracked from initial request to implementation using an auditable change management system. The platform is monitored for unauthorised changes on a regular/continuous basis using appropriate software tools.
27. There is a formal process in place for responding to/dealing with Security Incidents, which directly involves the Head of Operations and the CEO.
28. Cryptographic key information, unless encrypted or held in a tamper resistant environment, is kept in secure conditions under dual control of persons with split knowledge, unconnected with the sending and receiving of messages.
29. No passwords are transmitted or stored in clear at any time.

Client Data Protection

URIM do not keep paper, or other physical copies of client data. All data is stored on secure servers in secure data centres and all backups of client data are stored in encrypted format 'at rest'. URIM stands by its commitment to protect personally identifiable client information - including names, telephone numbers, pin numbers, passwords and any other personal information provided to us - and to keep the privacy promises and contractual data commitments made. Information is secured in accordance with GDPR legislation.

Data Disposal

Client data is encrypted at rest, so cannot be accessed directly from the physical devices on which it is stored. If a client's contract ends (or we receive an earlier formal client data removal request), then on the agreed day, all of their user data, historical reporting and database backups are immediately wiped from the Servers at each of URIM's hosting data centres. Once the data has been removed, the URIM account manager will notify the main contact at the registered client's organisation by telephone as well as in a concluding email confirmation message.

Data Protction

How Does Urim Safeguard My Data?

Urim App Limited
130 Old Street London
EC1V 9BD

Web: www.urim.app
Email: support@urimapp.com