SECURITY POLICY

Revision 2
21 March 2018

Document Control

Organisation	Content Catalyst Limited
Title	Security Policy
Author	Thomas Gibbs
Owner	Thomas Gibbs
Approved By	Thomas Gibbs
Available to	Company (MS Teams Team) members (whole company)
Versioning	Automated, backed up and controlled by SharePoint library

Table of Contents

Content Catalyst Ltd ("Content Catalyst") provides its hosted services through a Software-as-a-Service model. The hosted services and Customer data (including the Customer's website, database and associated files) are hosted by a third party supplier (currently Rackspace Inc.).

This document: (i) provides an overview of Content Catalyst's current processes and security measures relating to the hosted services; and (ii) describes Content Catalyst's security practices with respect to the hosted infrastructure – including the production websites and systems currently hosted by Rackspace Inc. This document includes Content Catalyst's own operating protocols together with those of Rackspace Inc.

More information regarding our hosting providers' certifications can be found at:

- Rackspace: https://www.rackspace.com/en-gb/compliance

The information in this Security Policy is provided in good faith for guidance only. The contents of this Security Policy are non-contractual and Content Catalyst accepts no liability for any claim arising out of or relating to the content or any breach of this Security Policy. This does not affect any terms and conditions in place with Content Catalyst, whether under a License Agreement, Subscription Services Agreement, NDA or other contractual document.

Where any conflict exists between the provisions in this Security Policy and the provisions within any contract with Content Catalyst (e.g. License Agreement, Subscription Services Agreement or NDA) the provisions within the contract with Content Catalyst will prevail.

This Security Policy may be amended by Content Catalyst at its discretion.

21 March 2018

Access Control

Group	Item
User IDs	User IDs are required to access information assets.
User Access and privileges	Information assets are only accessible to users whose job roles require that access (role-based access control), and only pending prior authorisation.
	There is a clear division between administrative tasks and user tasks, which are kept discrete.
	Any individual leaving the company or changing roles has access rights removed within 5 working days or fewer, preferably on the leaving day.
	Dedicated administration features are available to selected employees and can be used to assign read/write permissions to other users.
	All password reset requests are authenticated prior to processing, and care is taken to ensure they are always transmitted securely (e.g. that they are encrypted if sent over an unsecured network).
Passwords	Windows/system accounts and database accounts follow industry standard complexity requirements.
	System default passwords are changed or default users are disabled.
Authentication	Access to the highest classification levels requires the use of multi-factor authentication.
	Application, database and system administrative access requires username/password and IP match (whitelist) or VPN connection.
	Application administrative access is controlled by both Content Catalyst and the Customer.
	Database and system access controlled by Content Catalyst and Rackspace.
	A suite of proprietary APIs is available for performing remote access management and authentication.

Application & Interface Security

Group	Item
Software Change Management	Software changes are peer code-reviewed and tested by Content Catalyst's Quality Assurance team in an internal environment.
	Software changes are reviewed by relevant Content Catalyst stakeholders before moving to the production environment.
Software Development Life-Cycle	All software changes are code-reviewed by senior members of Content Catalyst's development team.
	All software changes are tested by the Quality Assurance team.
	All software changes are reviewed by the management team and by the appropriate stakeholders.
	Core features of the software are covered by a suite of automated code-level and user interface tests.
Security Development Life-Cycle	Content Catalyst's Security Development Lifecycle is based on Microsoft's SDL. More information regarding the security development life cycle in use may be made available on request at Content Catalyst's discretion.
Source Code Access	All development of core, web-based products is performed in-house at Content Catalyst's Leeds office.
Frameworks	iReports is built using the Microsoft .NET framework and benefits from the security features and ongoing patches made available by Microsoft.
Code Integrity	Measures are in place to prevent users from changing application code.
Data Integrity	Measures are in place to prevent users from changing data without proper authorization.
Penetration Testing	OWASP vulnerability scanning tools are in use as part of the Security Development Lifecycle.
	Port and network security scans are performed on a regular basis.

Asset Management

Group	Item
Asset Inventory	Physical assets are recorded in asset inventories.
	Assets are returned when individuals leave the company.
	An authorised software list is required for standard infrastructure configurations and is compiled if unavailable; if unauthorised or unlicensed software is identified then remediation is carried out.
Information labelling	Procedures are in place for information classification, labelling and handling. More information may be made available on request at Content Catalyst's discretion.

Business Continuity

Group	Item
Business Continuity Planning	A maintained, managed program of business continuity plans exists.
	Plans are regularly tested using a variety of techniques such as simulations, recovery testing and rehearsals.
	The hosting provider maintains detailed plans for data centres and all locations housing infrastructure and communication equipment which define how full information system recovery is carried out without compromising information security.
Data Portability	Data can be retrieved directly via the web application's API.

Compliance

Group	Item
Information Retention	Page loads are recorded by iReports.
	Activity is tracked against logins, which can be identified by user/IP.
	A schema ensures the logs are robust.
	Logs are not encrypted.
	Error logs are monitored remotely with action taken by Content Catalyst's Operations and QA teams as necessary.
General Data Protection Regulation (GDPR)	GDPR compliance is considered as part of both the Software and Security Development Lifecycles.

Cryptographic Mechanisms

Group	Item
Standards	Only approved cryptographic standards are used throughout the organisation.
	iReports passwords are hashed using the PBKDF2 system implemented with the RNGCryptoServiceProvider and Rfc2898DeriveBytes classes provided in .NET.
	iReports passwords are hashed before storage and not stored in plain text.
	All iReports communications containing passwords are performed over TLS.

HR Security

Group	Item
Preemployment	Employees are suitably qualified for their job roles. Where relevant, this includes having an appropriately specialist level of information security knowledge.
Employment	All employment contracts and consultant agreements include confidentiality and non-disclosure clauses to protect information assets and intellectual property, with disciplinary sanctions clearly defined and followed.

Operations Management

Group	Item
Configuration	Infrastructure configuration standards and standard operating procedures are implemented and regularly reviewed.
	System and device configurations include appropriate system hardening.
	Regular reviews are carried out for any changes made between environments.
	Specific development, test and production environments are maintained.
Anti-Malware	Anti-malware is required on all applicable infrastructure and all files from external sources are checked, including email attachments, download links, permitted software downloads and web traffic.
	Real-time malware scanning and reviews are performed against all system and user files on infrastructure and removable media.
	Antivirus definitions are automatically kept up-to-date.
Firewalls	Firewalls are implemented between networks where appropriate.
	Access to firewalls is monitored. Senior staff are alerted when firewall configuration is accessed or updated.
Wireless Networks	Internal wireless networks are restricted to authorised users only.
	Guest access is provided on a separate network.
Network Security	Access to network devices is actively managed; all ports, protocols, interfaces and security features that do not meet a business need are disabled by default.
	Network configurations are documented and maintained.
Network/System Segregation	Network segregation is standard practice between information assets of different classification levels or where risk assessment identifies the need for segregation.
Anti-Spam	Anti-spam mechanisms are in place and block, quarantine or alert.
Backup and Recovery	Information assets are backed up regularly.
	Backup media is stored off-site at a location providing the same or higher physical and environmental security standards as the original location housing the infrastructure and information being backed up.
	Automated tools are used to manage backups and regular testing of backup media and devices is carried out.
Monitoring	Automated tools are used to detect and alert on potential security issues.
	Individual job roles include responsibilities to respond to and remediate alerts.
Information Handling and Disposal	Assets are labelled according to their classification level.
	Secure disposal methods are required for all types of media.

	Electronic media disposal methods meet recognised industry standards for disposal.
	Where third parties are used for media disposal, certificates of destruction are obtained and filed.
Information Protection	No data can be written to removable media without approval.
	Responsibilities are clearly defined if removable media is taken off the premises.
	Records are maintained for removable media which is delivered to third parties.
	Non-removable media is encrypted according to the standards for cryptographic mechanisms relevant to the information classification level.
Segregation of Duties	Opportunities to misuse information assets are reduced by implementing segregation of duties throughout the organisation with focus on those roles with administration or privileged access and roles granting and managing access to information assets.
Vendor and Service Delivery	Third party organisations providing services are risk assessed prior to being contracted, and on a regular basis thereafter; service providers are required to demonstrate policies and standards which meet or exceed those of our company relative to the information assets for which services are being provided.
Support	24-hour emergency support is available for outages.
	Application-level support is provided during UK office hours.
Patch Management	Patches are manually applied by a member of the operations team (initially in a staging environment) and then immediately tested.
	All operating systems regularly patched.
	Network equipment is regularly patched.
	A failover site is available for extended periods of downtime due to patch application.
	Operating system vulnerability scanning is in place and carried out on a regular basis.
Autorun	Autorun features are disabled.

Physical Security for Hosted Infrastructure

Group	Item
Physical Access	Access is limited to authorized personnel.
	Badges and biometric scanning control access.
	Security cameras provide video surveillance.
	All physical facilities containing infrastructure and communications equipment are access controlled allowing only authorised individuals entry related to their specific role or task.
	Independent firms perform annual audits.
Environmental Access	Environmental Controls implemented to help mitigate against the risk of service interruption caused by fires, floods and other forms of natural disasters.
	Dual power paths into facilities.
	Uninterruptable power supplies (minimum N+1).
	On-site generators (minimum N+1) & service agreements with suppliers/
	HVAC (minimum N+1).
	Smoke detectors.
	Continuous facility monitoring.
	Utilities, services, emergency equipment and systems at all facilities meet appropriate regulations and are regularly maintained and tested.
	Facilities containing infrastructure and communications equipment are adequately heated and ventilated by air conditioning services.
Equipment Security	All devices are accessible only by authorised individuals.
	Devices are regularly maintained and may not be removed without prior authorisation.