World of Content

Security & Privacy Policies

S. Lit

202106-v1.1

Introduction

World of Content has created a series of policies to help us with data security and privacy. These policies are distributed to every workforce member and are regularly updated and expanded to reflect changes in the organization.

Some of these policies are adapted from the Datica HIPA Compliance Policies, which open sourced well documented and audited policies under a Creative Commons License.

Any questions regarding the following material can be directed towards the Security Officer:

Simon Lit
simon@worldofcontent.com

Note: The following document is an exported copy of our security and privacy policies and not the official version as distributed to the World of Content workforce.

Commonly Used Terms

- "Production Systems", systems that create, receive, store, or transmit user generated data.
- "Production Data", any data that resides on production systems.
- "Personal Data", any information that relates to an identified or identifiable living individual.
- "Third Party Companies", any party that is not registered as World of Content B.V. in The Netherlands, and include any associated (international) businesses like joint ventures, partner companies and contracted clients.
- "GDPR", General Data Protection Regulation.
- "Workforce Member", any individual that performs work for World of Content including but not limited to, employees, freelancers, and interns.
- "Security Officer", the highest authority on privacy and security.
- "Quality Management System", a system used for tracking and resolving issues. In our case this is Gitlab.
- "Customer", a representative of the contractually defined legal entity customer of one the World of Content created systems.
- "Partner", a representative of a legal entity sharing resources with World of Content. 1

Index

1. Data Classification Policy

1.1 Data Classification

1. Any system and its data is classified and documented in one of the following categories:
    - Secret: Reserved for sensitive data like personal information, user generated data, secrets, and access to critical systems. Access to secret data can only be granted by the highest security authority, the Security Officer in our case.
    - Confidential: Any company information that is not meant to be shared publicly, including, but limited to, source codes and usage statistics. Access to this data is contractually managed.
    - Public: Any information that is meant for the public domain, for example a blog article.

1.2 Risk Assessment

1. The Security Officer is responsible for granting access to Secret Data as explained in the Access Control Policy.
2. For every workforce member a risk assessment is created based on which information and systems the user has access to. This is managed and maintained by the Security Officer.
    - When assessing the risk someone poses of leaking, deleting or otherwise misusing secret or confidential information the Security Officer should create a distinction between read-only and update rights to this information.
    - Permanent deletion of secret and confidential information should not be possible without explicit permission of the Security Officer.

2. Access Control Policy

Access to World of Content systems and applications is limited for all users, including but not limited to employees, consultants, interns, and contracted partners. Access by any entity is always granted on a minimum necessary basis. These guidelines have been established to limit unauthorized access to any of the organization's systems.

2.1 Access Establishment

1. Requests for access to World of Content systems and applications are made formally using the following process:
2. A World of Content workforce member initiates the access request by creating an Issue in the World of Content Quality Management System.
    - User identities must be verified prior to granting access to new accounts.

    - ○ Identity verification must be done in person where possible; for remote employees, identities must be verified over the phone.
    - ○ For new accounts, the method used to verify the user's identity must be recorded on the Issue.
3. The Security Officer will grant access to systems as dictated by the employee's job title. If additional access is required outside of the minimum necessary to perform job functions, the requester must include a description of why the additional access is required as part of the access request.
4. Once the review is completed, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation. 5. If the review is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required. The Security Officer then grants requested access. ○ New accounts will be created with a temporary secure password that meets all requirements from Password Management in §2.5, which must be changed on the initial login.
    - ○ All password exchanges must occur over an authenticated channel. ○ All password exchanges must either be secured by end-to-end encryption or the password must be split and exchanged using at least two different channels.
    - ○ Access grants are accomplished by leveraging the access control mechanisms built into the systems. Account management for non-production systems may be delegated to a workforce member at the discretion of the Security Officer.
6. Access is not granted until receipt, review, and approval by the Security Officer.
7. The request for access is retained for future reference.
8. All access to World of Content systems and services is reviewed and updated on a bi-annual basis to ensure proper authorizations are in place commensurate with job functions.

9. Access to production systems is controlled using centralized user management and authentication.
10. Temporary accounts are not used unless absolutely necessary for business purposes.
    - ○ Accounts are reviewed every 90 days to ensure temporary accounts are not left unnecessarily.
    - ○ Accounts that are inactive for over 90 days are removed.
11. All application to application communication using service accounts is restricted and not permitted unless absolutely needed. Automated tools are used to limit account access across applications and systems.
12. Access is granted through encrypted, VPN tunnels that utilize two-factor authentication.
    - ○ Two-factor authentication is accomplished using a Time-based One-Time Password (TOTP) as the second factor.

    - VPN connections use 256-bit AES 256 encryption, or equivalent.
    - VPN sessions are automatically disconnected after 30 minutes of inactivity.

13. In cases of increased risk or known attempted unauthorized access, immediate steps are taken by the Security Officer to limit access and reduce risk of unauthorized access.
14. Direct system to system, system to application, and application to application authentication and authorization are limited and controlled to restrict access.

2.2 Person or Entity Authentication

1. Role based access categories for each World of Content system and application are pre-approved by the Security Officer, or an authorized delegate of the Security Officer.
2. World of Content utilizes hardware and software firewalls to segment data, prevent unauthorized access, and monitor traffic for denial of service attacks.
3. Each workforce member has and uses a unique user ID and password that identifies him/her as the user of the information system.
4. Generic or shared accounts are not allowed on any of the World of Content systems.
5. Each Customer and Partner has and uses a unique user ID and password that identifies him/her as the user of the information system.
6. All Customer support desk interactions must be verified before support personnel will satisfy any request having information security implications.
7. Passwords requirements mandate strong password controls (see below) and are not displayed or transmitted in plain text at any time.

2.3 Employee Workstation Use

All workstations at World of Content are company owned:

1. Workstations may not be used to engage in any activity that is illegal or is in violation of organization's policies.
2. Information systems/applications also may not be used for any other purpose that is illegal, unethical, or against company policies or contrary to organization's best interests.
3. Solicitation of non-company business, or any use of organization's information systems/applications for personal gain is prohibited.

2.4 Employee Termination Procedures

1. The Human Resources Department (or other designated department), users, and their supervisors are required to notify the Security Officer upon completion and/or termination of access needs and facilitating completion of the "Termination Checklist".
2. The Human Resources Department, users, and supervisors are required to notify the Security Officer to terminate a user's access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report): ○ The user has been using their access rights inappropriately;
    ○ A user's password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password);
    ○ An unauthorized individual is utilizing a user's User Login ID and password (a new password may be provided to the user if the user is not identified as providing the unauthorized individual with the User Login ID and password).
3. The Security Officer will terminate users' access rights immediately upon notification, and will coordinate with the appropriate workforce member to terminate access to any non-production systems managed by those employees.
4. The Security Officer audits and may terminate access of users that have not logged into the organization's information systems/applications for an extended period of time.

2.5 Password Management

1. User IDs and passwords are used to control access to World of Content systems and may not be disclosed to anyone for any reason.
2. Users may not allow anyone, for any reason, to have access to any information system using another user's unique user ID and password.
3. On all production systems and applications in the World of Content environment, and where supported, password configurations are set to require:
    ○ a minimum length of 8 characters;

    ○ a mix of uppercase characters, lower case characters, and numbers or special characters;
    ○ a 90-day password expiration, or 60-day password expiration for administrative accounts;
    ○ prevention of password reuse using a history of the last 6 passwords; ○ where supported, modifying at least 4 characters when changing passwords; 4. 2 Factor Authentication (2FA) must be enabled where possible. The authentication factors could be:
    ○ Passwords;
    ○ Security tokens;
    ○ USB sticks with a secret token;

- Biometrics;

5. All system and application passwords must be stored and transmitted securely.
   - Where possible, passwords should be stored in a hashed format using a salted cryptographic hash function (SHA-256 or equivalent).
6. Passwords are inactivated immediately upon an employee's termination (refer to the Employee Termination Procedures in §2.4).
7. All default system and application passwords are changed before deployment to production.
8. Upon initial login, users must change any passwords that were automatically generated for them.
9. Password change methods must use a confirmation method to correct for user input errors.
10. All passwords used in configuration scripts must be environment based, and securely stored.
11. If a user believes their user ID has been compromised, they are required to immediately report the incident to the Security Officer.

3. Personal Data Processing Policy

3.1 Data Protection

● Personal Data is classified as "Confidential". See Data Classification Policy §1. ● World of Content must comply with the European data protection law and principles outlined in the General Data Protection Regulation(“GDPR”), which means that personal data is:

- Collected only for valid and documented purposes and not used in any way

that is incompatible with those purposes;
    - Accurate and kept up to date;
    - Stored only for as long as necessary;
    - Kept securely and protected against unauthorized access;
    - Protected against loss or destruction using appropriate technical and organizational measures;
- The organization ensures that any associate or employee having to access personal information:
    - Have received appropriate training on their responsibilities;
    - Have all their actions logged and available for auditing;

3.2 Data Storage

- Installation of Personal Data on systems not owned by World of Content must be approved by the Customer or Partner and the Security Officer.
- If not done prior to transmittal, Personal Data should be scrubbed immediately upon storage, to eliminate storage of data not related to the originally purpose of processing.
- Personal Data must be stored in a manner that ensures it is sufficiently segregated from other data, to ensure proper access controls.
- Hard disks containing Personal Data must use disk level encryption consistent with current industry best practices.
- All systems housing Personal Data must have active anti-virus protection. ● Members of the World of Content workforce must not store Personal Data on their company workstation or mobile device.

3.3 Data Access

Requesting and granting access to any of the World of Content systems is outlined in the Access Control Policy.

3.4 Data Transfers

When personal data has to be processed by third party companies, for Error Tracking or Usage Statistics for example, we have to send that data to the servers of that third party company. These cases are outlined below:

3.4.1 Non Restricted Transfers

Transferring personal data to Third Party Companies within the EEA, including but not

limited to user ids, emails, and names, is regulated under the GDPR. For these transfers the following rules apply:

- Active members of the EEA are listed here.
- Data transfers to a company within the EEA is only allowed in the following circumstances:
    - Incidental data transfers are allowed only if approved by the Security Officer.
    - Regular data transfers are only allowed to one the approved tools as described in Approved Tools Policy §6.1.
- The Security Officer is responsible for receiving permission from the user for the data transfer, whether contractually or explicitly by receiving written consent. ● Data transfers are only allowed when a Data Processing Addendum is in place. More information about DPA's can be found here.
- Data transfers for both incidental and regular data transfers are documented on:
    - Company details including name and country;
    - Date (or date range if regular);
    - General description of the data;
    - Reason for transferring data;
- Data transfers contain only the minimum required data to adequately perform the intended action by the third party.

3.4.2 Restricted Transfers

A transfer of personal data outside the protection of the GDPR (which we refer to as a 'restricted transfer'), most often involves a transfer from inside the EEA to a country outside the EEA. For these transfers we maintain the following guidelines:

- On top of the policy outlines as described in §3.4.1 of this document, data can only be transferred if approved by the following process:
    - Do we need to make a restricted transfer of personal data in order to meet our purposes? If no, the transfer without any personal data is approved. ○ Has the EU made a positive 'adequacy decision' in relation to the country or territory where the receiver is located or a sector which covers the receiver? If yes, the transfer is approved.
    - Have we put in place one of the 'appropriate safeguards' referred to in the GDPR? If yes, the transfer is approved.

    - Does an exception provided for in the GDPR apply? If yes, the transfer is approved.
    - If none of the questions found a provision which permits the restricted transfer, then that restricted transfer is not approved in accordance with the GDPR.

Note: since the US-EU Privacy Shield is no longer valid as of July 2020, the USA is

not deemed adequate.

3.5 Data Retention

All personal data and user generated data is retained for the duration of the contract, which is usually a year over year recurring contract. After the contract has expired data will be deleted within one month but might remain in our backups for a maximum of one year. We collect the following data with the following reasons:

- Functional data, like products, exports, account data from my.worldofcontent.com; ○ This is the data the users stores in our database to use our primary services. ○ Data will remain in backups for one year after deletion.
- System logs, every time the user triggers an action like export, image resize, etc. a log is created with detailed information about the request;
  - ○ We use these logs for finding bugs and performance issues. We don't store any information about the user, but filenames might reference user generated data.
  - ○ These logs automatically expire after 1 month
- System errors, every time an exception occurs we log detailed information about that and previous requests;
  - ○ We use these logs for finding and resolving bugs. We don't store any information that is relatable to a specific user, but we might reference a model id that is created by a user. For example if the client created a product and something went wrong, we might reference the id or name of that product in one of our logs.
  - ○ The bugs are auto resolved after one year.

4. Data Integrity Policy

World of Content takes data integrity seriously. We strive to assure data is protected from unauthorized access and that it is available when needed. The following policies drive many of our procedures and technical settings in support of the World of Content mission of data protection.

4.1 Monitoring

1. All access to Production Systems are logged. This is done following the Auditing Policy.
2. All alterations to Production Data, whether this is done directly in the database or by users of any of the World of Content systems, are also logged according to the Auditing Policy.

4.2 Patch Management

1. Software patches and updates will be applied to all systems in a timely manner. In the case of routine updates, they will be applied after thorough testing. In the case of updates to correct known vulnerabilities, priority will be given to testing to speed the time to production. Critical security patches are applied within 30 days from testing and all security patches are applied within 90 days after testing.

4.3 System Security

1. All Production Systems must disable services that are not required to achieve the business purpose or function of the system.
2. Production systems are monitored using IDS systems. Suspicious activity is logged and alerts are generated.
3. Vulnerability scanning of Production Systems must occur on a predetermined, regular basis, no less than annually. Currently this is done during every production and development build (at least once per day). Scans are reviewed by the Security Officer, and retained for future reference.
4. System, network, and server security is managed and maintained by the Security Officer in conjunction with the Dev Ops team.
5. Up-to-date system lists and architecture diagrams are kept for all production environments.

4.4 Production Data Security

1. Appropriate safeguards are in place to reduce the risk of compromise of production data, this includes but is not limited to:

    - Review controls designed to protect Production Data from improper alteration or destruction;
    - Access logs are available for Production Data and automated monitoring is in place for potential security incidents;
    - Personal data is segmented and only accessible to workforce members

authorized to access data;

2. All Production Data is stored on encrypted disks, backups are also encrypted before transmission.

4.5 Vulnerability Scanning

World of Content is proactive about information security and understands that vulnerabilities need to be monitored on an ongoing basis. World of Content has multiple systems in place to pro-actively find and resolve security vulnerabilities.

1. We use the following tools for automatically finding security vulnerabilities during production and development builds:
    - Gitleaks. Gitleaks is a SAST tool for detecting hardcoded secrets like passwords, api keys, and tokens in git repos. Gitleaks aims to be the easy-to-use, all-in-one solution for finding secrets, past or present, in your code.
    - ESLint Security. This project will help identify potential security hotspots, but finds a lot of false positives which need triage by a human.
    - PHPCS Security Audit. phpcs-security-audit is a set of PHP_CodeSniffer rules that finds vulnerabilities and weaknesses related to security in PHP code.
    - Amazon ECR image scanning. Amazon ECR image scanning helps in identifying software vulnerabilities in your container images. Amazon ECR uses the Common Vulnerabilities and Exposures (CVEs) database from the open source Clair project and provides you with a list of scan findings.
2. If new vulnerabilities are found during review, the process outlined below is used to test those vulnerabilities. Once those steps are completed, the Issue is then reviewed again.
3. Once the review is completed, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review.
4. If the review is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.
5. In the case of new vulnerabilities, the following steps are taken:
    - All new vulnerabilities are verified manually to assure they are repeatable. Those not found to be repeatable are manually tested after the next vulnerability scan, regardless of if the specific vulnerability is discovered again.

- Vulnerabilities that are repeatable manually are documented and reviewed by the Security Officer to see if they pose a serious risk. Based on the risk assessment the security vulnerability is mitigated in a timely manner.

6. Penetration testing is performed regularly as part of the World of Content vulnerability

management policy.
○ External penetration testing is performed annually by a third party. ○ Internal penetration testing is performed quarterly. Below is the process used to conduct internal penetration tests.
■ The Security Officer initiates the penetration test by creating an Issue in the World of Content Quality Management System.
■ The Security Officer, or a Security Engineer assigned by the Security Officer, is assigned to conduct the penetration test.
■ Gaps and vulnerabilities identified during penetration testing are reviewed, with plans for correction and/or mitigation, by the Security Officer before the Issue can move to be approved.
■ Once the testing is completed, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further testing and review.
■ If the Issue is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.
7. This vulnerability policy is reviewed on a quarterly basis by the Security Officer.

4.6 Backup Policy and Procedures

1. All data in World of Content production systems are backed up daily. 2. The World of Content Dev Ops Team is designated to be in charge of backups. 3. Dev Ops Team members are trained and assigned to complete backups and manage the backup media.
4. Backups are securely encrypted and stored in a manner that protects them from loss or environmental damage.
5. Backups are annually tested to make sure that files can be successfully restored. 14

5. Auditing Policy

World of Content safeguards the confidentiality, integrity, and availability of data, applications, systems, and networks in order to ensure business continuity and client trust. Therefore it will audit access and activity to detect, report, and guard against:

- Network vulnerabilities and intrusions;
- Breaches in confidentiality and security;
- Performance problems and flaws in applications;
- Improper alteration or destruction of user generated data;
- Out of date software and/or software known to have vulnerabilities.

5.1 Auditing Policies

1. Responsibility for auditing information system access and activity is assigned to the World of Content Security Officer. The Security Officer shall:

    - Assign the task of generating reports for audit activities to the workforce member responsible for the application, system, or network;
    - Assign the task of reviewing the audit reports to the workforce member responsible for the application, system, or network, to the Security Officer, or any other individual determined to be appropriate for the task;
    - Organize and provide oversight to a team structure charged with audit compliance activities (e.g., parameters, frequency, sample sizes, report formats, evaluation, follow-up, etc.).

2. World of Content auditing processes shall address access and activity at the following levels listed below. Auditing processes may address date and time of each log-on attempt, date and time of each log-off attempt, devices used, functions performed, etc.

    - User: User level audit trails generally monitor and log all commands directly initiated by the user, all identification and authentication attempts, and data and services accessed.
    - Application: Application level audit trails generally monitor and log all user activities, including data accessed and modified and specific actions. ○ System: System level audit trails generally monitor and log user activities, applications accessed, and other system defined specific actions.
    - Network: Network level audit trails generally monitor information on what is operating, penetrations, and vulnerabilities.

3. World of Content shall log all incoming and outgoing traffic to into and out of its environment. This includes all successful and failed attempts at data access and editing. Data associated with this data will include origin, destination, time, and

other relevant details that are available to World of Content.

4. World of Content's Security Officer is authorized to select and use auditing tools that are designed to detect network vulnerabilities and intrusions. Such tools are

explicitly prohibited by others, including other workforce members, without the explicit authorization of the Security Officer. These tools may include, but are not limited to:

- ○ Scanning tools and devices;
- ○ Password cracking utilities;
- ○ Network "sniffers".
- ○ Passive and active intrusion detection systems.

5. The process for review of audit logs, trails, and reports shall include:

   ○ Description of the activity as well as rationale for performing the audit. ○ Identification of which World of Content workforce members will be responsible for review (workforce members shall not review audit logs that pertain to their own system activity).
   ○ Frequency of the auditing process.
   ○ Determination of significant events requiring further review and follow-up. ○ Identification of appropriate reporting channels for audit results and required follow-up.

6. Vulnerability testing software may be used to probe the network to identify what is running (e.g., operating system or product versions in place), whether publicly-known vulnerabilities have been corrected, and evaluate whether the system can withstand attacks aimed at circumventing security controls.

   ○ Testing may be carried out internally or provided through an external third-party vendor. Whenever possible, a third party auditing vendor should not be providing the organization IT oversight services (e.g., vendors providing IT services should not be auditing their own services - separation of duties).
   ○ Testing shall be done on a routine basis, currently monthly.

7. Software patches and updates will be applied to all systems in a timely manner as described in Data Integrity §4.2.

5.2 Audit Requests

1. A request may be made for an audit for a specific cause. The request may come

from a variety of sources including, but not limited to the Security Officer, as workforce member or an application user.

2. A request for an audit for specific cause must include time frame, frequency, and nature of the request. The request must be reviewed and approved by World of Content's Security Officer.

5.3 Review and Reporting of Audit Findings

1. Audit information that is routinely gathered must be reviewed in a timely manner by the responsible workforce member(s).
2. The Security Officer initiates the log review by creating an Issue in the World of Content Quality Management System.
3. The Security Officer, or a member of World of Content DevOps team assigned by the Security Officer, is assigned to review the logs.
4. Relevant audit log findings are added to the Issue; these findings are investigated in a later step. Once those steps are completed, the Issue is then reviewed again. 5. Once the review is completed, the Security Officer approves or rejects the Issue. Relevant findings are reviewed at this stage. If the Issue is rejected, it goes back for further review and documentation. The communications protocol around specific findings are outlined below.
6. If the Issue is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.
7. The reporting process shall allow for meaningful communication of the audit findings to those workforce members, Customers, or Partners requesting the audit. ○ Significant findings shall be reported immediately in a written format. World of Content's security incident response form may be utilized to report a single event.
    ○ Routine findings shall be reported to the sponsoring leadership structure in a written report format.
8. Reports of audit results shall be limited to internal use on a minimum necessary/need-to-know basis. Audit results shall not be disclosed externally without administrative and/or legal counsel approval.
9. Security audits constitute an internal, confidential monitoring practice that may be included in World of Content's performance improvement activities and reporting. Care shall be taken to ensure that the results of the audits are disclosed to administrative level oversight structures only and that information which may further expose organizational risk is shared with extreme caution.
10. Whenever indicated through evaluation and reporting, appropriate corrective actions must be undertaken. These actions shall be documented and shared with the responsible workforce members.

5.4 Audit Log Security Controls and Backup

1. Audit logs shall be protected from unauthorized access or modification, so the

information they contain will be made available only if needed to evaluate a security incident or for routine audit activities as outlined in this policy.
2. All audit logs are protected in transit and encrypted at rest to control access to the content of the logs.

5.5 Workforce Training, Education, Awareness and Responsibilities

1. World of Content workforce members are provided training, education, and awareness on safeguarding the privacy and security of business and Personal Data. World of Content's commitment to auditing access and activity of the information applications, systems, and networks is communicated through new employee orientation, ongoing training opportunities and events, and applicable policies. World of Content workforce members are made aware of responsibilities with regard to privacy and security of information as well as applicable sanctions/corrective disciplinary actions should the auditing process detect a workforce member's failure to comply with organizational policies.

5.6 External Audits of Information Access and Activity

1. Prior to contracting with an external audit firm, World of Content shall:
    - ○ Outline the audit responsibility, authority, and accountability;
    - ○ Choose an audit firm that is independent of other organizational operations;
    - ○ Ensure technical competence of the audit firm staff;
    - ○ Require the audit firm's adherence to applicable codes of professional ethics;
    - ○ Assign organizational responsibility for supervision of the external audit firm.

6. Approved Tools Policy

World of Content uses a set of tools used by members of the workforce. These software tools are either self-hosted, with security managed by World of Content, or they are hosted by a Subcontractor with appropriate business associate agreements in place to preserve data integrity. These tools and the approval of new tools are outlined below.

6.1 Approved Tools

- **Gitlab**. GitLab is an open source tool built on top of Git and is hosted and secured by World of Content. It is utilized for storage of configuration scripts and other infrastructure automation tools, as well as for source and version control of application code.
- **Google Suite**. Google Suite is used for email exchange, file storage, calendars, and document collaboration.
- **Sentry**. Sentry is a service for tracking exceptions in production environments. ● **Mailgun**. Mailgun is a service for sending and receiving emails from code. This is used to automatically notify users of World of Content built services when certain actions are performed.
- **Google Analytics**. Google Analytics is used to track usage statistics of World of content services.
- **MailChimp**. MailChimp is used for communicating in bulk with all World of Content associates, employees, and users.
- **Amazon Web Services**. Amazon Web Services is used for hosting the infrastructure of all World of Content created systems demanding high availability.
- **Hetzner**. Hetzner is used for hosting the infrastructure of systems used by World of Content.
- **Slack**. Slack is used as the main business communication channel. ● **UptimeRobot**. UptimeRobot is used to detect if all internet facing apps are responding.
- **Jira**. Jira is used for technical support, e.g. for reporting a bug.

6.2 Tool Approval

1. When using a new tool to process confidential or secret data, the tool must be approved by the Security Officer. Tools are only approved when:
    - The tool is deemed required or critical for business continuity;
    - When a Data Processing Addendum is in place;
    - When the data is only processed in the EEA. If this is not the case the transfer of data automatically falls into the "Restricted Transfer" category. Data can only be transferred if it is compliant with Personal Data Processing §3.4.2;

2. All tools are reviewed before and during use to detect, report, and guard against any form of misuse as described in Auditing Policy §5.1 (Hereafter: "flaw") according to the following interval:
    - ○ After the finding of a flaw;
    - ○ On a quarterly basis;
3. Reviewing tools as well as further investigation into discovered flaws is the responsibility of the Security Officer. Tools are investigated regularly for the following flaws:
    - ○ User accounts compliance according to Access Control Policy; ○ Personal data processing compliance according to Personal Data Processing Policy;
    - ○ Data integrity compliance according to Data Integrity Policy;
4. Approved tools are added to the list above and to the "System Access Control Overview" document by the Security Officer or approved delicate.

7. Configuration and Change Management Policy

World of Content standardizes and automates configuration and deployments using different tools for security scanning, change log creations, infrastructure upgrades, and scalability settings. These are described in the policy below:

7.1 Configuration Management Policies

1. All World of Content production infrastructure is hosted using Amazon Web Services (AWS).
2. No systems are deployed into AWS environments without approval of the Head of Development and the Security Officer.
3. All changes to production systems, network devices, and firewalls are approved by the Security Officer before they are implemented to assure they comply with security requirements.
4. The configuration of systems deployed to AWS are managed by CloudFormation:
    - CloudFormation templates are stored in a central repository;
    - All procedures as described in Software Development Procedures §7.4 apply;
5. All changes to production systems are tested before they are implemented in production.
6. Implementation of approved changes are only performed by members of the World of Content workforce.
7. All frontend functionality (developer dashboards and portals) is separated from backend (database and app servers) systems by being deployed on separate servers or containers.
8. All software and systems are tested using appropriate testing techniques, which include unit tests, end to end tests, and integration tests.
9. World of Content utilizes development and staging environments that mirror production to assure proper function.
10. All committed code is reviewed using merge requests to assure software code quality and proactively detect potential security issues in development.

7.2 Provisioning Production Systems

1. Before provisioning any systems, Dev Ops team members must file a request in the World of Content Quality Management System.
2. The Head of Development, or an authorized delegate, must approve the provisioning request before any new system can be provisioned, an exception to this is the provisioning of new instances of an existing system for scalability.
3. Once provisioning has been approved, the Dev Ops team member can configure the new system.

4. Once the system has been provisioned, the ops team member must contact the Security Officer to inspect the new system. The Security Officer or a delegate will verify that baseline security measures have been applied including, but not limited to, verifying the following items:
    - Removal of default users used during provisioning.
    - Network configuration for system.
    - Data volume encryption settings.
    - Intrusion detection and virus scanning software installed.
5. The new system may be rotated into production once the Head of Development and Security Officer verify all the provisioning steps listed above have been correctly followed and has marked the Issue with the "Approved" state.

7.3 Changing Existing Systems

1. Subsequent changes to already-provisioned systems are handled by updating CloudFormation templates, and can only be performed by members of the Dev Ops team.
2. Configuration changes must be initiated by creating a Merge Request in GitLab.
3. In all cases, before rolling out the change to production, the change must be checked by the Security Officer or an approved delegate.
4. Once the request has been approved by the Security Officer or an approved delegate, the Dev Ops team member may roll out the change into production environments.

7.4 Software Development Procedures

1. All development uses feature and hotfix branches based on the main development branch for the current release. Any changes required for a new feature or defect fix are committed to that branch.
    - These changes must be covered under 1) a unit test where possible, or 2) integration tests.
    - Integration tests are required if unit tests cannot reliably exercise all facets of the change.
2. Developers are strongly encouraged to follow the commit message conventions suggested by GitHub.
    - Commit messages should be wrapped to 72 characters.
    - Commit messages should be written in the present tense. This convention matches up with commit messages generated by commands like git merge and git revert.
3. Once the feature and corresponding tests are complete, a merge request will be created using the GitLab web interface. The merge request should indicate which

feature or defect is being addressed and should provide a high-level description of the changes made. Before merging, merge request must:
    - Not have any unresolved issues or comments;
    - Be approved by at least one other team member when deploying to Development;
    - Be approved by the Security Officer or an approved delegate, and a Senior Developer when deploying to Staging or Production;
4. Merge request must always link one or multiple Issues which it tends to resolve, each issue must have labels indicating the nature of the issue.
5. Code reviews are performed as part of the merge request procedure. Once a change is ready for review, the author(s) will notify other engineers using an appropriate mechanism, typically via an "@channel" message in Slack.
    - Other members of the development team will review the changes, using the guidelines above.
    - Members of the development team should note all potential issues with the code; it is the responsibility of the author(s) to address those issues or explain why they are not applicable.

7.5 Software Builds

- All environment specific builds of World of Content systems containing application code must be stored for at least 6 months and contain at least:
    - The environment target;
    - An increasing and unique version or build number;
    - A change log;
    - Any artifacts containing information about security vulnerabilities;

8. Incident Response Policy

World of Content implements an information security incident response process to consistently detect, respond to, and report incidents, minimize loss and destruction, mitigate the weaknesses that were exploited, and restore information system functionality and business continuity as soon as possible.
The incident response process addresses:

- Continuous monitoring of threats through intrusion detection systems (IDS) and other monitoring applications;
- Establishment of an information security incident response team;
- Establishment of procedures to respond to media inquiries;
- Establishment of clear procedures for identifying, responding, assessing, analyzing, and follow-up of information security incidents;
- Workforce training, education, and awareness on information security incidents and required responses; and
- Facilitation of clear communication of information security incidents with internal, as well as external, stakeholders.

8.1 Incident Management Policies

The World of Content incident response process follows the process recommended by SANS, an industry leader in security. Process flows are a direct representation of the SANS process which can be found below.

1. **Events** - Any observable computer security-related occurrence in a system or network with a negative consequence. Examples:

- Hardware component failing causing service outages.
- Software error causing service outages.
- General network or system instability.

2. **Precursors** - A sign that an incident may occur in the future. Examples:
    - Monitoring system showing unusual behavior.
    - Audit log alerts indicated several failed login attempts.
    - Suspicious emails targeting specific World of Content staff members with administrative access to production systems.
3. **Indications** - A sign that an incident may have occurred or may be occurring at the present time. Examples:
    - Antivirus alerts for infected files.
    - Excessive network traffic directed at unexpected geographic locations.
4. **Incidents** - A violation of computer security policies or acceptable use policies, often resulting in data breaches. Examples:
    - Unauthorized disclosure of Personal Information.
    - Unauthorized change or destruction of Personal Information.
    - A data breach accomplished by an internal or external entity.

    - A Denial-of-Service (DoS) attack causing a critical service to become unreachable.

World of Content workforce members must report any unauthorized or suspicious activity seen on production systems or associated with related communication systems (such as email or Slack). In practice this means keeping an eye out for security events, and letting the Security Officer know about any observed precursors or indications as soon as they are discovered.

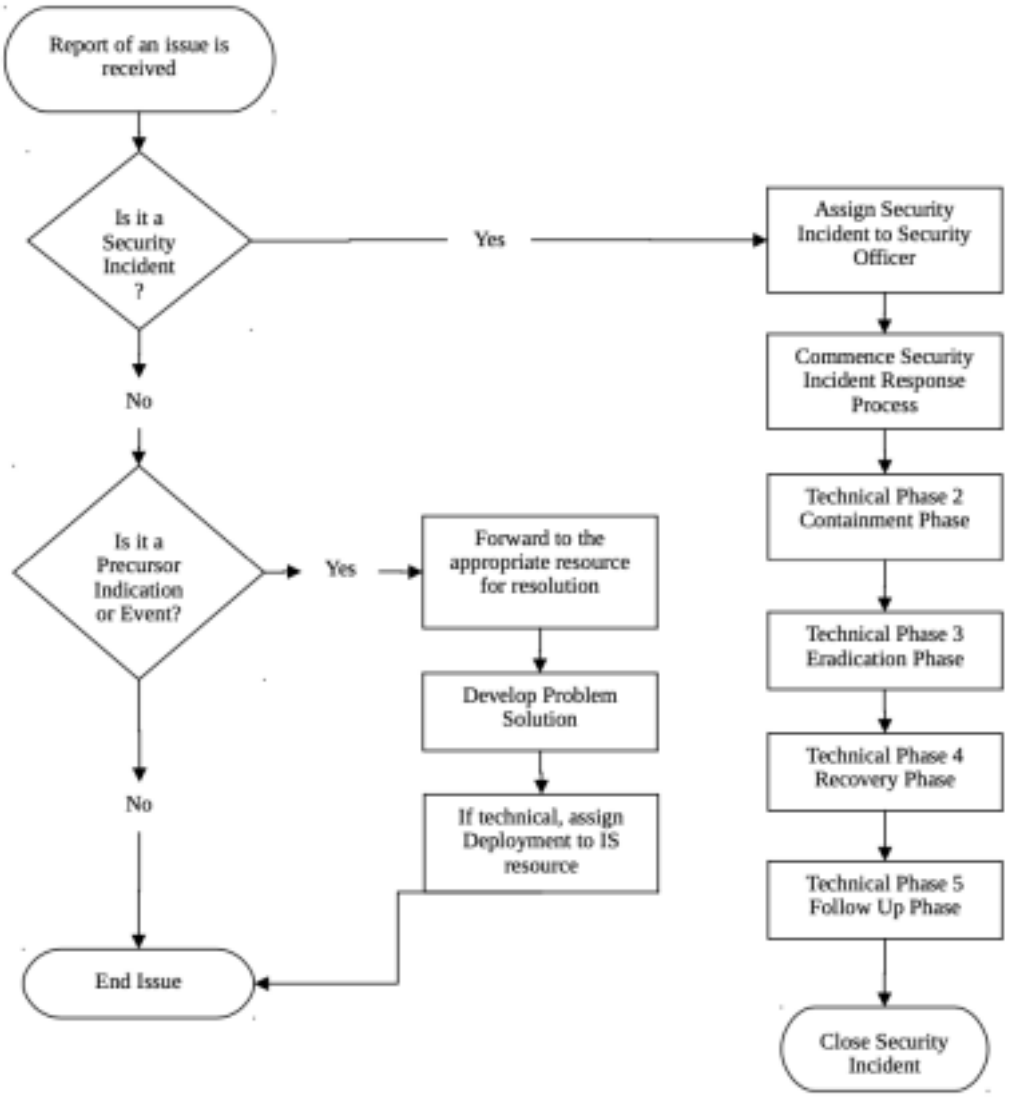

Figure 1: A representation of the SANS process.

8.2.1 Identification Phase

1. Immediately upon observation World of Content members report suspected and known Events, Precursors, Indications, and Incidents in one of the following ways: 1. Direct report to management, the Security Officer, or other;

2. Email;
3. Phone call;
4. Slack;
5. Anonymously through workforce member's desired channels;

2. The Security Officer determines if the issue is an Event, Precursor, Indication, or Incident.

1. If the issue is an event, indication, or precursor the Security Officer forwards it to the appropriate resource for resolution.
2. If the issue is a security incident the Security Officer activates the Security Incident Response Team (SIRT) and notifies the Head of Development. 1. If a non-technical security incident is discovered the SIRT completes the investigation, implements preventative measures, and resolves the security incident.
2. Once the investigation is completed, progress to Phase V, Follow-up.
3. If the issue is a technical security incident, commence to Phase II: Containment.
4. The Containment, Eradication, and Recovery Phases are highly technical. It is important to have them completed by a highly qualified technical security resource with oversight by the SIRT team.
5. Each individual on the SIRT and the technical security resource document all measures taken during each phase, including the start and end times of all efforts.
6. The lead member of the SIRT team facilitates initiation of a SIR Form supplied by the Security Officer. The intent of the SIR form is to provide a summary of all events, efforts, and conclusions of each Phase of this policy and procedures.

3. The Security Officer notifies any affected Customers and Partners. If no Customers and Partners are affected, notification is at the discretion of the Security Officer. 4. In the case of a threat identified, the Security Officer is to form a team to investigate and involve necessary resources, both internal and potentially external.

8.2.2 Containment Phase (Technical)

In this Phase, World of Content's IT department attempts to contain the security incident. It is extremely important to take detailed notes during the security incident response process. This provides that the evidence gathered during the security incident can be used successfully during prosecution, if appropriate.

1. The SIRT reviews any information that has been collected by the Security Officer or any other individual investigating the security incident.
2. The SIRT secures the network perimeter.
3. The IT department performs the following:
    1. Securely connect to the affected system over a trusted connection. 26
    2. Retrieve any volatile data from the affected system.
    3. Determine the relative integrity and the appropriateness of backing the system up.
    4. If appropriate, back up the system.
    5. Change the password(s) to the affected system(s).
    6. Determine whether it is safe to continue operations with the affected

system(s).

7. If it is safe, allow the system to continue to function;
    1. Complete any documentation relative to the security incident on the SIR Form.
    2. Move to Phase V, Follow-up.
8. If it is NOT safe to allow the system to continue operations, discontinue the system(s) operation and move to Phase III, Eradication.
9. The individual completing this phase provides written communication to the SIRT.

4. Continuously apprise the Head of Development of progress.
5. Continue to notify affected Customers and Partners with relevant updates as needed

8.2.3 Eradication Phase (Technical)

The Eradication Phase represents the SIRT's effort to remove the cause, and the resulting security exposures, that are now on the affected system(s).

1. Determine symptoms and cause related to the affected system(s). 2. Strengthen the defenses surrounding the affected system(s), where possible (a risk assessment may be needed and can be determined by the Security Officer). This may include the following:
    1. An increase in network perimeter defenses.
    2. An increase in system monitoring defenses.
    3. Remediation ("fixing") any security issues within the affected system, such as removing unused services/general host hardening techniques.
3. Conduct a detailed vulnerability assessment to verify all the holes/gaps that can be exploited have been addressed.
    1. If additional issues or symptoms are identified, take appropriate preventative measures to eliminate or minimize potential future compromises.
4. Update the documentation with the information learned from the vulnerability assessment, including the cause, symptoms, and the method used to fix the problem with the affected system(s).
5. Apprise the Head of Development of the progress.
6. Continue to notify affected Customers and Partners with relevant updates as needed.
7. Move to Phase IV, Recovery.

8.2.4 Recovery Phase (Technical)

The Recovery Phase represents the SIRT's effort to restore the affected system(s) back to operation after the resulting security exposures, if any, have been corrected. 1. The technical team determines if the affected system(s) have been changed in any way.

1. If they have, the technical team restores the system to its proper, intended

functioning ("last known good").

2. Once restored, the team validates that the system functions the way it was intended/had functioned in the past. This may require the involvement of the business unit that owns the affected system(s).
3. If operation of the system(s) had been interrupted (i.e., the system(s) had been taken offline or dropped from the network while triaged), restart the restored and validated system(s) and monitor for behavior.
4. If the system had not been changed in any way, but was taken offline (i.e., operations had been interrupted), restart the system and monitor for proper behavior.
5. Update the documentation with the detail that was determined during this phase.
6. Apprise the Head of Development of progress.
7. Continue to notify affected Customers and Partners with relevant updates as needed.
8. Move to Phase V, Follow-up.

8.2.5 Follow-up Phase (Technical and Non-Technical)

The Follow-up Phase represents the review of the security incident to look for "lessons learned" and to determine whether the process that was taken could have been improved in any way. It is recommended all security incidents be reviewed shortly after resolution to determine where response could be improved. Timeframes may extend to one to two weeks

post-incident.

1. Responders to the security incident (SIRT Team and technical security resource) meet to review the documentation collected during the security incident. 2. Create a "lessons learned" document and attach it to the completed SIR Form. 1. Evaluate the cost and impact of the security incident to World of Content using the documents provided by the SIRT and the technical security resource.
    2. Determine what could be improved.
    3. Communicate these findings to the Head of Development for approval and for implementation of any recommendations made post-review of the security incident.
    4. Carry out recommendations approved by the Head of Development; sufficient budget, time and resources should be committed to this activity. 5. Close the security incident.

8.2.6 Periodic Evaluation

It is important to note that the processes surrounding security incident response should be periodically reviewed and evaluated for effectiveness. This also involves appropriate training of resources expected to respond to security incidents, as well as the training of the workforce regarding the organizations expectation for them, relative to security responsibilities. The incident response plan is tested annually.