2024/03/01

# DATA SECURITY TERMS - RELATIVITYONE GOVERNMENT

## I. DEFINITIONS

Capitalized terms used in these Data Security Terms but not defined have the meanings set forth in the Master Terms and Conditions or the applicable Order.

## II. CLOUD VENDOR DATA SECURITY CONTROLS

Relativity uses a cloud vendor ("Cloud Vendor") to provide the infrastructure environment to run Relativity's RelativityOne Government product. The current Cloud Vendor is Microsoft Azure Government. Accordingly, RelativityOne Government currently operates within Cloud Vendor's security framework. Details on Cloud Vendor's security, privacy, and compliance standards may be found on the Microsoft Azure Trust Center homepage: https://azure.microsoft.com/en-us/support/trust-center/. Relativity reserves the right to switch to a different Cloud Vendor or to a data center that Relativity or its affiliate operates, provided (a) the data security arrangements shall be at least consistent with prevailing industry standards and the provisions in these Data Security Terms and the security of Customer Data shall not be materially diminished; and (b) Relativity will provide at least 90 days' advance notice to Customer of any change in Cloud Vendor. Current Cloud Vendor security compliance offerings include, but are not limited to, FedRAMP High Authority to Operate (ATO), DoD Impact Levels 2, 4, and 5, CJIS, International Traffic in Arms Regulations, and Defense Federal Acquisition Regulation Supplement Clause 252.204-7012. As part of the process for obtaining and maintaining these compliance offerings, the Cloud Vendor has implemented numerous procedures, including but not limited to: (a) personnel background checks and security awareness training; (b) physical and logical access control safeguards; (c) incident response plans; and (d) disaster recovery and business continuity plans.

## III. AUTHORIZED USER ACCESS AND PERMISSIONS

Within RelativityOne Government, Customer's Admins can choose from numerous local and external identification authentication methods and resource options to help secure the process of granting, controlling and revoking user access. Admins can also view case access and permission audits to ensure that Authorized Users accessing RelativityOne Government have the proper level of permissions. RelativityOne Government's object security model means that Admins can manage varying levels of security for objects such as views, tabs, and fields, across Customer's Geo and in each workspace. RelativityOne's group permission model allows Admins to quickly apply or modify security profiles for a number of Authorized Users simultaneously by assigning permissions at group level. After configuring a group's access permissions, Admins can preview the effective security rights by impersonating a general member of the group or a specific user. More details on such permission controls are included in Relativity's Documentation.

## IV. RELATIVITY DATA SECURITY PROCEDURES

### 1. OVERVIEW

While no business can prevent all potential hacking or other criminal conduct, and the Cloud Vendor for RelativityOne Government has certified infrastructure safeguards, Relativity also maintains its own security program with administrative, technical, and physical safeguards. Relativity's security program, together with the Cloud Vendor's security program, is designed to:

- protect the confidentiality, integrity and availability of Customer Data in Relativity's possession or control or to which Relativity has access in RelativityOne Government;
- protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Customer Data;

- protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Customer Data;
- protect against accidental loss or destruction of, or damage to, Customer Data; and
- safeguard Customer Data as required by any Laws which apply to Relativity based on Relativity's operations in processing Customer Data.

Without limiting the generality of the foregoing, Relativity's security program, which is in addition to the Cloud Vendor's security program, currently includes the elements described in Sections 2 through 17 below.

## 2. SECURITY CERTIFICATIONS AND AUDITS.

Relativity shall maintain during the course of the Term (as amended) a FedRAMP Moderate ATO validated by a Third-Party Assessment Organization for its RelativityOne Government offering. RelativityOne Government Customers can review Relativity's ATO status via the method as required by FedRAMP. Additionally, Relativity will complete a reasonable data security questionnaire relating to Relativity's current operation of RelativityOne Government.

## 3. SECURITY TRAINING, CONFIDENTIALITY OBLIGATIONS AND BACKGROUND CHECKS

Relativity provides a mandatory security and privacy awareness and training program for all Relativity employees and any persons working as contractors who may have access to Customer Data in the performance of their services (collectively, "Workers With Access"). All Workers With Access are also subject to confidentiality obligations. Further, Relativity conducts background checks consistent with prevailing practices for similar companies in connection with the hiring or engaging of all Workers With Access. Relativity will not hire or engage any Worker With Access if the background check shows that the individual was convicted of a crime involving theft, dishonesty, fraud or computer-related crimes. Relativity's commitments with respect to background checks are subject to all applicable Laws pertaining to such background checks. Relativity workforce members with direct access to RelativityOne Government may have an additional requirement of Relativity Workers With Access to Customer Data receiving a Public Trust Background Screening administered by Relativity's Authorizing Official.

## 4. ENCRYPTION PROGRAMS

### 4.1 Encryption Policy

Relativity has a documented security cryptography policy that dictates encryption use, applicable encryption standards, and encryption strength.

### 4.2 Encryption in Transit

Encryption in transit utilizing standard encryption technology (e.g., Transport Layer Security (TLS), IPSec, and SMB).

### 4.3 Email Encryption

RelativityOne Government has a default setting so that email messages between Customer and Relativity are encrypted leveraging Transport Layer Security (TLS). Encryption technology used adheres to applicable legal requirements governing the use of such technology. Email messages to Customer's Authorized Users who do not use Customer's email domain are encrypted by Opportunistic TLS.

### 4.4 Encryption at Rest\

All Customer Data at rest is encrypted using industry standard symmetric encryption.

## 5. ANTI-MALWARE SERVICES

Relativity leverages third-party anti-malware program services to help protect against malware impacting system services and functions, as further described below.

- Relativity provides, supports and maintains an anti-malware service
- Relativity's anti-malware service is configured to automatically scan files that are accessed by RelativityOne
- Government servers and storage services by untrusted processes (the process itself is scanned).
- Relativity's anti-malware service is configured to log all scanning activity. Upon the detection of a suspected malware infected file, Relativity's anti-malware service is configured to automatically quarantine the infected file and generate an associated log entry.

## 6. PHYSICAL SECURITY

Relativity maintains locked perimeter doors and requires that personnel use electronic key cards and other reasonable measures designed to ensure that physical access to the Relativity premises is limited to properly authorized individuals. The Cloud Vendor maintains physical access security controls for the data center, including layers of defense-in-depth security that include perimeter fencing, video cameras, security personnel, secure entrances, and real-time communications networks.

## 7. DATA DISPOSAL

Customer may delete or export Customer Data from the SaaS Product from time to time in Customer's discretion and will do so in any event at the end of the Subscription Term for the applicable Order. Upon receiving Customer's written request to decommission a Geo, Relativity will follow the secure deletion or disposal procedures in its applicable standard operating procedures any remaining Customer Data contained in the decommissioned Geo, the associated disaster recovery Geo in the back-up data center and any related media. Deletion or disposal means the Customer Data is rendered inaccessible, undecipherable or otherwise unrecoverable, provided that Relativity may retain copies of Customer Data in accordance with the RelativityOne Government Disaster Recovery and Business Continuity Plans, or as otherwise necessary to perform its obligations under the Agreement. Relativity may retain platform monitoring, usage and performance metrics, and security logs, none of which include Customer Data.

## 8. OTHER ACCESS CONTROLS

As further described under Section 9 (Access Control and Password Management Policy), Relativity has policies, procedures, and logical controls designed to limit access to RelativityOne Government to properly authorized personnel on a "need to know" basis, to prevent those personnel who should not have access from obtaining access and to remove access of personnel on a timely basis in the event of a change in job responsibilities or job status. For those personnel who are granted access to RelativityOne Government, Relativity's standard operating procedures further limit such access to resolving issues with system components rather than viewing any Customer Data (except in situations when incidental viewing of Customer Data may be required in connection with resolving an issue or responding to a Customer request). Relativity logs such access for at least one (1) year (the first 90 days of which is in readily available hot status, and the remainder of which is in cold storage), and will make such logs available to Customer for review to the extent those logs reveal access to Customer Data.

## 9. ACCESS CONTROL AND PASSWORD MANAGEMENT POLICY

### 9.1 General RelativityOne Government Password Requirements

Relativity has an Access Control and Password Management Policy, and an automated password management system to enforce the policy requirements. The policy covers all applicable systems, applications, and databases. There are classes of password use in Relativity's enterprise and RelativityOne Government as further detailed below. Industry standard prevailing password practices are deployed to protect against unauthorized use of passwords, including: (a) minimum password length; (b) password complexity; (c) password history; (d) password lockout for failed password attempts; and (e) randomly generated initial passwords.

### 9.2 Relativity Enterprise Identity and Password Management

The Relativity enterprise uses a single sign-on multi-factor authentication service (currently Okta) for authenticating all individuals in the organization and for authenticating access to the systems that support and operate RelativityOne Government (the "Back-End").

(a) **RelativityOne Government Front-End Access.** Relativity employs the RelativityOne Government following methods respecting access to the user interface (User Interface (also referred to as the "Front-End"):

- Customer controls Front-End logins to its Geo through a password management system that employs the user authentication provider, e.g., Active Directory. Customer controls RelativityOne Government Front-End password policies for Customer's Authorized Users, and can choose from any supported authentication provider in RelativityOne Government including length, expiration, reuse, and complexity requirements, lockout, and reset options.
- Relativity supports integration with OIDC and some SAML Single Sign-On providers to restrict the access through the Front-End.
- Relativity personnel who need Front-End access as systems administrators are subject to a gating arrangement consisting of technical and organizational controls designed to prevent such personnel from accessing Customer Data without Customer's consent.

(b) **RelativityOne Government Back-End Access.** Relativity employs the following methods respecting access to the Back-End:

- All TCP connections to Back-End RelativityOne Government resources are brokered through a privileged access management solution, which logs the unique user ID that created the connections. Only members of specific Relativity Active Directory groups can access Back-End RelativityOne Government accounts through the privileged access management solution, and all access to this solution requires authentication through a single sign-on multi-factor authentication service (currently Okta). When Relativity personnel access the RelativityOne Government Back-End, they use shared system and application accounts to authenticate to RelativityOne servers. Relativity has RelativityOne Government administrative controls in place to manage risks from the use of such shared system and application accounts and to track such usage. With this privileged access management system, Authorized Users cannot see the credentials; they only launch the TCP connections.
- Relativity service accounts are used by the system to run Back-End processes for RelativityOne Government, and may require occasional access by Relativity personnel for support and maintenance on a limited need-to-know basis, e.g., to restart a stuck processing worker agent process. Any such access requires a properly credentialed

log-in. Relativity has technical and administrative controls in place to manage risks from the use of shared IDs and to track such usage.

## 10. DISASTER RECOVERY AND BUSINESS CONTINUITY PLANS

The Cloud Vendor and Relativity have disaster recovery and business continuity plans in place, and Relativity has established RTO and RPO timelines as set forth in the Service Level Terms. These plans include a separate back-up data center (which may be in a separate country) and a formal framework by which an unplanned event will be managed to minimize the loss of vital resources. The formal framework includes a defined back-up policy and associated procedures, including documented policies and procedures designed to: (a) perform back-up of Customer Data to a separate back-up data center in a scheduled and timely manner; (b) provide effective controls to safeguard backed-up Customer Data; (c) securely transfer Customer Data to and from the back-up location; and (d) fully restore applications and operating systems; (e) demonstrate periodic testing of restoration from the back-up location. If Relativity makes back-ups to tape or other removable media, all such back-ups shall be encrypted in compliance with the encryption requirements set forth above.

## 11. ASSIGNED SECURITY RESPONSIBILITY

Relativity assigns responsibility for the development, implementation, and maintenance of its security program, including:

- designating a security official with overall responsibility;
- defining security roles for individuals with security responsibilities;
- performing risk assessments of Relativity and RelativityOne Government at least annually and whenever major changes to systems or processes occur; and
- designating a Security Governance Committee consisting of cross-functional management representatives to meet on a regular basis.

## 12. SECURE CODING PRACTICES

All Relativity developer personnel are required to take a course in security awareness and secure coding, and Relativity's coding standards have a strong security component. Among other things, the OWASP Secure Coding Practices Reference are integrated into Relativity's coding standards. The coding standards are reviewed annually and maintained by the architecture and security teams to remain up to date and enforce the prevailing standards. Standard production source code changes go through a pull request workflow to ensure peer review for code quality and adherence to coding standards. Each commit into a Relativity code base requires an approval from another engineer. The approver reviews for compliance with Relativity's coding standards prior to accepting any code change. For new features, completion of a structured review process with Relativity's security team is required. During this process, each project receives a risk rating based on risk ranking criteria. The higher the risk rating, the more security scrutiny the project is subject to during its lifecycle.

## 13. SECURITY TESTING

Relativity regularly tests the key controls, systems and procedures of its security program to validate that they are properly implemented and effective in addressing the threats and risks identified. Testing currently includes:

- Internal risk assessments
- Network configuration tests

- Use of internal security specialists and/or a third party to conduct web application level security assessments. These assessments generally test for the OWASP Top 10, which may include the following:
    - Cross-site request forgery
    - Improper input handling (e.g., cross-site scripting, SQL injection, XML injection, cross-site flashing)
    - XML and SOAP attacks
    - Weak session management
    - Data validation flaws and data model constraint inconsistencies
    - Insufficient authentication
    - Insufficient authorization
    - Web application penetration testing:
        - During web application penetration testing, a dedicated penetration testing team looks for security suspects, such as XSS, Cross Site Request Forgery, authentication issues, and authorization issues. Relativity uses industry-standard tests alongside specialized tests, sometimes customized for new features. The penetration testing team also leverages other penetration testing techniques based on their disparate experiences and knowledge of RelativityOne Government.
        - On an annual basis, Relativity engages an external penetration testing firm for an extensive test covering the functionality RelativityOne Government, including industry standard tests like those from the Open Web Application Security Project (OWASP), and additional tests that the penetration testing firm deems necessary as it explores the application.
        - Upon request, Relativity will provide Customer with an annual penetration test results as part of its Annual Assessment and lists them through the Office of Management Business MAX Information System (OMB Max) or any equivalency as specified under applicable Laws.

## 14. SECURITY MONITORING & AUTOMATED VULNERABILITY SCANS

Relativity monitors network and production systems, including error logs on servers, disks and security events for any suspicious or malicious activities. Monitoring generally includes:

- Arranging for automated vulnerability scans of any assets deployed in RelativityOne Government containing Customer Data, to be performed periodically to identify, mitigate or remediate any vulnerabilities. All scan results are uploaded at least monthly onto OMB Max, or any equivalency as specified under applicable Laws.
- Subscribing to vulnerability intelligence services or to information security advisories and other relevant sources providing current information about system vulnerabilities (none of which involves the submission of any Customer Data).
- Reviewing changes affecting systems handling authentication, authorization, and auditing;
- Reviewing privileged Back-End access to RelativityOne Government to validate privileged

access is appropriate.

- Engaging a validated Third Party Assessor Organization (3PAO) to perform network vulnerability assessments and penetration testing on at least an annual basis.
- Maintaining industry standard event logging for servers, applications, and networking equipment to facilitate security incident and event management. Relativity maintains such logs for at least one (1) year (the first 90 days of which is in readily available hot status, and the remainder of which is in cold storage).
- Classifying vulnerabilities in accordance with industry standard risk rating methodologies (e.g., the Common Vulnerability Scoring System, OWASP, or NIST).
- Mitigating, and/or remediating vulnerabilities in RelativityOne Government infrastructure or applications that could allow direct unauthorized access to Customer Data, whether by applying an available patch or taking other reasonable actions, in the following time frames:

| **Severity** | **Policy** | |
|---|---|---|
| | **Relativity SaaS Product** | **Third-Party Software** |
| **Critical** | Before the software is released if found in release testing. Within 7 days of identification of vulnerability if found after release. | Within 7 days of receiving notice of patch availability from the third-party vendor and up to 15 days for testing. |
| **High** | Before the software is released if found in release testing. Within 30 days of identification of vulnerability if found after release. | Within 30 days of receiving notice of patch availability from the third-party vendor and up to 60 days for testing. |
| **Medium** | Within 90 days of identification of vulnerability. | Within 90 days of receiving notice of patch availability from the third-party vendor and up to 60 days for testing. |
| **Low** | Within 180 days of identification of vulnerability. | Within 180 days of receiving notice of patch availability from the third-party vendor and up to 60 days for testing. |

## 15. RELATIVITYONE GOVERNMENT CHANGE AND CONFIGURATION MANAGEMENT.

Relativity maintains policies and procedures for managing changes to RelativityOne Government policies and procedures include:

- a process for documenting, testing and approving the promotion of changes into production; and
- a security patching process that requires patching systems in a timely manner based on a risk

analysis.

## 16. SECURITY INCIDENT RESPONSES

### 16.1 Cyber Team

Relativity has a Cyber Team that: (a) is capable of meeting on short notice to address any incidents;, and (b) focuses on continuous development and improvement of procedures to be followed in the event of any security breach of RelativityOne Government Customer Data or any security breach of any application or system directly associated with the accessing, processing, storage, communication or transmission of RelativityOne Government Customer Data. Procedures currently include:

- Roles and responsibilities: Relativity's Cyber Team will act in coordination with additional security and engineering resources throughout the incident response process;.
- Investigation: assessing the risk the incident poses and determining who may be affected;
- Communication: internal reporting as well as the Data Breach notification process set forth below;
- Recordkeeping: keeping a permanent record of what was done and by whom to help in later analysis and possible legal action; and
- Audit: conducting and documenting root cause analysis and remediation plans.

### 16.2 Security Incident Response

(a) **Notification of a Data Breach.** Unless notification is delayed or prohibited by the actions or demands of a law enforcement agency, Relativity will report a data breach to Customer's security contact designated to Relativity within 24 hours following determination by Relativity that such an incident has occurred, or that Relativity reasonably suspects may have occurred. "Data Breach" means: (i) the unauthorized acquisition, access, use, disclosure, or destruction or impairment of Customer Data that Relativity determines has occurred; or (ii) the unauthorized acquisition, use, disclosure, or destruction or impairment of Customer Data that Relativity reasonably suspects may have occurred but which it cannot definitively conclude occurred.

(b) **Relativity Response.** Relativity will take reasonable measures to promptly mitigate the cause of any Data Breach, implement any appropriate monitoring protocol, and identify the circumstances that allowed the Data Breach to happen in order to help prevent any further similar Data Breaches (unless the Data Breach was caused by the acts or omissions of Customer or any of its authorized users which Customer authorizes to access RelativityOne Government, in which case Customer shall take such actions). Relativity may work with forensic investigators, law firms and law enforcement agencies to help determine the nature, extent and source of any Data Breach and may make any disclosures of security records, security logs and other information that Relativity deems appropriate or is required to make under applicable Laws (provided any disclosures of Customer Data shall require Customer's prior written consent, except to the extent that Relativity would risk fines or other sanctions or liabilities for withholding the information). If Relativity makes any statements about a Data Breach without the approval of Customer, Relativity will not disclose that Customer or Customer Data was involved, unless such disclosure is required by applicable Law.

(c) **Cooperation with Customer.** Upon Customer's request, Relativity will cooperate with Customer (and Customer's regulators and insurers) to investigate the Data Breach and seek

to identify the specific Customer Data involved in the Data Breach (without charge, except to the extent the Data Breach was caused or contributed to by the acts or omissions of Customer or any Authorized User which Customer authorizes to access RelativityOne Government). Unless prohibited by applicable Law, Relativity will: (i) provide information regarding the nature and consequences of the Data Breach as such information is collected or otherwise becomes available to Relativity; and (ii) otherwise reasonably assist Customer to notify affected individuals, government agencies, regulators and/or credit bureaus; provided the parties agree that Customer is solely responsible for determining whether to notify impacted owners of the Customer Data and if regulatory bodies or enforcement commissions applicable to Customer or Customer Data need to be notified, and for providing such notices.

(d) **Access Credentials.** Customer is responsible for safeguarding its Access Credentials and promptly notifying Relativity of any known or reasonably suspected unauthorized use of any Access Credentials.

## 17. ADJUSTMENT TO THESE DATA SECURITY TERMS

Relativity monitors and evaluates its security program on a regular basis and may adjust it and these Data Security Terms from time to time, as appropriate in light of: (a) prevailing practices; (b) any relevant changes in technology and any internal or external threats to Relativity or the Customer Data; and/or (c) Relativity's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.