

PERFORCE® GLIFFY INFORMATION SECURITY TERMS

These Information Security Terms (“**Security Terms**”) supplement the Gliffy EULA for Plugins on Atlassian Jira and Confluence between Gliffy and Client (the “**EULA,**” and together with these Security Terms, the “**Agreement**”). The EULA is hereby amended to incorporate this Security Supplement as part of the Agreement; notwithstanding any integration or merger clause in Section 10 of the EULA or elsewhere, this Security Supplement forms part of the Agreement between the parties. Capitalized terms not defined herein shall have the meanings set forth in the EULA. In the event of any conflict between these Security Terms and the EULA, the EULA shall control, except that with respect to Gliffy’s security obligations, these Security Terms shall control to the extent they impose obligations on Gliffy that are more specific than any general warranty disclaimer or limitation in the EULA.

We will ensure that our third-party providers, suppliers, agents, and subcontractors that provide Software to Client comply with the applicable provisions of these Security Terms. We will implement appropriate technical and organizational security measures based on applicable Industry Standards and Data Protection Laws. Client may access Gliffy security certifications and audit reports at Perforce Trust Center (trust.perforce.com), upon acknowledging a nondisclosure agreement, as provided on the Trust Center.

1. **ADDITIONAL DEFINITIONS**

The following definitions apply to these Security Terms:

“**Affiliates**” means, with respect to a party, any entity that directly or indirectly controls, is controlled by, or is under common control with such party, where “control” means the ownership of more than fifty percent (50%) of the voting securities or equivalent voting interests of such entity.

“**Client**” means the individual or entity that has agreed to the EULA, referred to as “You” in the EULA.

“**Confidential Information**” means any non-public information disclosed by one party to the other in connection with the Agreement that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and circumstances of disclosure, including without limitation Client Content, security audit reports, and information regarding Gliffy’s security practices.

“**Content**” means any information, materials, or works in any medium or format, including without limitation documents, data, databases, text, graphics, audio files, video files, photographs, images, illustrations, software code, three-dimensional models, designs, and any other digital or electronic materials.

“**Client Content**” means all Content (as defined in the EULA) that Client or its authorized users upload, input, transmit, or otherwise make available through the Software, together with any results, outputs, or derivatives that Client or its authorized users generate using the Software. Client Content does not include: (a) Third-Party Content; (b) any materials proprietary to Gliffy, its Affiliates, or their licensors that are incorporated into or made accessible through the Software; or (c) client contact information, including but not limited to names, email addresses, telephone numbers, mailing addresses, or similar contact details of Client’s employees, contractors, end users, or other representatives.

“**Data Protection Laws**” means all applicable laws, regulations, and binding guidance relating to the processing, privacy, and protection of personal data, including without limitation the General Data Protection Regulation (EU) 2016/679, the California Consumer Privacy Act, and any successor legislation or implementing regulations.

“**Gliffy Product**” means the Software and any other Gliffy-branded software products or services made available by Gliffy to Client under the Agreement or any related agreement.

“**Industry Standard(s)**” means those commercially reasonable security measures designed to ensure the security of the Software provided to Client and include standard technical and organizational security measures to ensure the security, integrity, and confidentiality of Client Content and to protect against the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Client Content. We will comply with applicable Data Protection Laws to ensure that Client Content, as it is provided to Gliffy, is not destroyed (except as expressly permitted under the Agreement), lost, altered, corrupted, or otherwise impacted such that it is not readily usable by Client in its business operations.

“**Security Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to Client Content that we transmit, store or otherwise process in providing the Software.

“**Software**” means the Gliffy software plugins for Atlassian Jira and Confluence licensed to Client under the EULA, as defined in the EULA.

“**Third-Party Content**” means any Content, data, software, applications, services, materials, or other information that is provided, made available, or accessible by or from any third party (including but not limited to third-party vendors, service providers, licensors, or other entities that are not Gliffy or its Affiliates) through, in connection with, or as part of any Software, including without limitation any Content that may be integrated with, linked to, or accessible through the Software or Atlassian’s cloud or server environments. Third-Party Content is not owned, controlled, endorsed, or maintained by Gliffy or its Affiliates and may be subject to separate terms and conditions imposed by the applicable third party.

2. **INFORMATION SECURITY POLICIES AND MEASURES**

- 2.1. **Policies.** Gliffy’s senior management will document and approve our information security policies.
- 2.2. **Review of the Policies.** We will review our information security policies at least annually, or promptly after material changes are made to the policies to confirm applicability and effectiveness. We will not make changes to the policies that would materially degrade our security obligations.
- 2.3. **Information Security Reviews.** We will independently review our approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) at planned intervals or when significant changes occur.
 - 2.3.1. **Business Continuity.** During the term of the Agreement, we will maintain a business continuity (BC) or high availability (HA) solution and related plan that is consistent with Industry Standards. In addition, the solution and related plan will ensure:
 - 2.3.2. that installed systems used to provide Software will be restored in case of interruption; we can restore the availability and access to Client Content in a timely manner in the event of a physical or technical incident; and
 - 2.3.3. the ongoing confidentiality, integrity, availability, and resilience of systems we use to provide Software.
- 2.4. **Testing.** We will maintain a process for regularly testing the effectiveness of our technical and organizational measures for ensuring the security of the processing of Client Content.

3. **INFORMATION SECURITY FRAMEWORK**

- 3.1. **Security Accountability.** We will assign one or more security officers who will be responsible for coordinating and monitoring all information security functions, policies, and procedures.
- 3.2. **Security Roles and Responsibility.** Gliffy personnel, contractors, and agents who provide Offerings will have confidentiality agreements with Gliffy.
- 3.3. **Risk Management.** We will perform appropriate information security risk assessments as part of an ongoing risk governance program with the following objectives:
 - 3.3.1. recognize risk;
 - 3.3.2. assess the impact of risk;
 - 3.3.3. where risk reduction or mitigation strategies are identified and implemented, effectively manage the risk with recognition that the threat landscape constantly changes.

4. **HUMAN RESOURCE SECURITY**

- 4.1. **Security Training.** We will provide appropriate security awareness, education, and training to all our personnel and contractors who have access to the Software we provide Client.

- 4.2. **Background Screening.** We will ensure that background checks have been performed on personnel who are part of teams managing our hosting infrastructure. We will perform background checks in accordance with applicable law and our background screening policies and procedures. We will only allow individuals who have passed background checks to be part of teams managing our hosted infrastructure.

5. **ASSET MANAGEMENT**

- 5.1. We will maintain an asset inventory of all media and equipment where Client Content is stored. We will restrict access to that media and equipment to our authorized personnel. We will prevent the unauthorized reading, copying, modification, or removal of data media.
- 5.2. We will classify Client Content so that it is properly identified and will appropriately restrict access to it. Specifically, we will ensure that no person we appoint to process Client Content will do so unless that person:
 - 5.2.1. has a need to access Client Content for the purpose of performing our obligations under the Agreement;
 - 5.2.2. has been authorized by Gliffy in a manner consistent with our information security policies;
 - 5.2.3. has been fully instructed by us in the procedures relevant to performing our obligations under the Agreement, in particular the limited purpose of processing Client Content; and
 - 5.2.4. is aware that they are prohibited from copying any Client Content transmitted by you to Gliffy, provided, however, that we may retain copies of Client Content you provide us under the Agreement on our servers for backup and archive purposes until completion of the Agreement.
- 5.3. We will maintain measures to ensure that persons we appoint to process Client Content will prevent the unauthorized input of Client Content and the unauthorized inspection, modification, or deletion of stored Client Content.
- 5.4. We will implement procedures to ensure Client Content is only allowed on Gliffy approved systems which require multi-factor authentication. Client Content is never allowed to be transferred to external systems, devices or other storage systems.
- 5.5. **Security of Software Components.** We agree to appropriately inventory all software components (including open-source software) used with the Software. We will assess whether any components have any security defects and/or vulnerabilities that could lead to unauthorized disclosure of Client Content. We will perform an assessment prior to delivery of, or providing Client access to, the Software and on an ongoing basis during the term of the Agreement. We agree to remediate any security defect or vulnerability we detect in a timely manner.

6. **ACCESS CONTROL**

- 6.1. **Policy.** We will maintain an appropriate access control policy that is designed to restrict access to Client Content and Gliffy assets to authorized personnel, agents, and contractors. All references to user accounts and passwords in this Section relate only to Gliffy's users, user accounts, and passwords. Section 6 does not apply to Client's access to and use of the Software, Client's user accounts, or Client's passwords.
- 6.2. **Authorization.**
 - 6.2.1. We will maintain user account creation and deletion procedures for granting and revoking access to all assets, Client Content, and all Perforce internal applications while providing Software under the Agreement. We will assign an appropriate authority to approve creation of user accounts or elevated levels of access for existing accounts.
 - 6.2.2. We will maintain and update records of employees and contractors who are authorized to access systems that are involved in providing Software to Client and review such records regularly. Administrative and technical support personnel, agents, or contractors will only be permitted to have access to such data when required and only if they comply with our applicable technical and organizational measures.
 - 6.2.3. We will ensure the uniqueness of user accounts and passwords for everyone. Individual user accounts will not be shared.

6.2.4. We will remove access rights of personnel and contractors to assets that store Client Content upon termination of their employment, contract, or agreement as soon as possible, but no later than the end of the next business day, or adjust access upon change of personnel role.

6.3. **Authentication.**

6.3.1. We will use Industry Standard capabilities to identify and authenticate personnel, agents, and contractors who attempt to access information systems and assets.

6.3.2. We will maintain Industry Standard practices to deactivate passwords that have been corrupted or disclosed.

6.3.3. We will monitor for repeated access attempts to information systems and assets.

6.3.4. We will maintain Industry Standard password protection practices that are designed to maintain the confidentiality and integrity of passwords generated, assigned, distributed, and stored in any form.

6.3.5. We will use multi-factor authentication for all administrative access, including domain and cloud portal administrative access. Multi-factor authentication may include techniques such as the use of cryptographic certificates, OTP tokens, or biometrics.

6.4. **Data-processing Equipment.**

6.4.1. We will deny unauthorized persons access to systems and equipment used for processing Client Content ("**Data-processing Equipment**").

6.4.2. We will prevent the use of automated Data-processing Equipment by unauthorized persons using data communication equipment.

6.4.3. We will ensure that persons authorized to use automated Data-processing Equipment only have access to the Client Content covered by their access authorization.

6.4.4. We will ensure that it is subsequently possible to verify and establish which Client Content has been put into automated Data-processing Equipment, when it was added, and by whom the input was made.

7. **CRYPTOGRAPHY**

7.1. We will maintain policies and standards regarding the use of cryptographic controls that we implement to protect Client Content. Such protections will include the pseudonymization and encryption of Client Content, as further detailed below in Section 9. We will implement Industry Standard key management policies and practices designed to protect encryption keys for their entire lifetime.

8. **PHYSICAL AND ENVIRONMENTAL SECURITY**

8.1. **Physical Access to Facilities.** We will limit access to facilities where systems that are involved in providing the Software are located to identified personnel, agents, and contractors.

8.2. **Protection from Disruptions.** We will use reasonable efforts, and if within our control, protect equipment from power failures and other disruptions caused by failures in supporting utilities.

8.3. **Secure Disposal or Reuse of Equipment.** We will verify that all Client Content has been deleted or securely overwritten from equipment containing storage media using Industry Standard processes prior to disposal or reuse.

9. **OPERATIONS SECURITY**

9.1. **Operations Policy.** We will maintain appropriate operational and security operating procedures and we will make them available to all Gliffy personnel who require them.

9.2. **Protections from Malware.** We will maintain anti-malware controls that are designed to protect systems from malicious software, including malicious software that originates from public networks.

- 9.3. **Configuration Management.** We will have policies that govern the development, testing, and release of software updates and utilities for the Software.
- 9.4. **Change Management.** We will maintain and implement procedures to ensure that only approved and secure versions of the code, configurations, systems, and applications will be deployed in production environment(s).
- 9.5. **Encryption of Data.** We will deploy encryption solutions with no less than 256-bit Advanced Encryption Standard (“AES”) encryption.
- 9.6. **Systems.** We will ensure that the functions of the systems used to provide Software perform, that the appearance of faults in the functions is reported, and that stored Client Content cannot be corrupted by means of a malfunctioning of such systems.

10. **COMMUNICATIONS SECURITY**

10.1. **Information Transfer.**

10.1.1. To the extent Client Content is transmitted to or processed by Gliffy systems in connection with the Software, such Client Content is encrypted in-transit and at rest. We will use Industry Standard encryption to encrypt Client Content.

10.1.2. We will restrict access through encryption to Client Content stored on media that is physically transported from our facilities.

10.1.3. We will ensure that it is possible to verify and establish the extent to which Client Content has been or may be transmitted or made available using data communication equipment.

10.2. **Security of Network Services.** We will ensure that Industry Standard security controls and procedures for all network services and components are implemented whether such services are provided in-house or outsourced.

10.3. **Intrusion Detection.** We will deploy intrusion detection or intrusion prevention systems for all systems used to provide Software to Client to provide continuous surveillance for intercepting and responding to security events as they are identified and we will update the signature database as soon as new releases become available for commercial distribution.

10.4. **Firewalls.** We will have appropriate firewalls in place to only allow documented and approved ports and services to be used. All other ports will be in a deny-all mode.

11. **SYSTEM ACQUISITION, DEVELOPMENT, AND MAINTENANCE**

11.1. **Workstation Encryption.** We will require hard disk encryption of at least 256-bit AES on all workstations and/or laptops used by personnel, contractors, and agents where such personnel are accessing or processing Client Content.

11.2. **Application Hardening.**

11.2.1. We will maintain and implement secure application development policies, procedures, and standards that are aligned to Industry Standard practices such as the SANS Top 25 Security Development Techniques or the OWASP Top Ten project.

11.2.2. All personnel responsible for secure application design, development, configuration, testing, and deployment will be qualified to perform the Offerings and receive appropriate training regarding our secure application development practices.

11.3. **System Hardening.**

11.3.1. We will perform periodic (at least quarterly) access reviews for system administrators for all supporting systems requiring access control.

11.3.2. We will implement patching tools and processes for both applications and operating system software. When outdated systems can no longer be patched, we will update to the latest version of application

software. We will remove outdated, unsupported, and unused software from the system.

11.3.3. We will limit administrative privileges to only those personnel who have both the knowledge necessary to administer the operating system and a business need to modify the configuration of the underlying operating system.

11.4. **Infrastructure Vulnerability Scanning.** We will scan our internal environment (e.g., servers, network devices, etc.) related to the Software at least monthly and our external environment related to the Software at least weekly. We will have a defined process to address any findings and will ensure that any high-risk vulnerabilities are addressed no later than 30 days after discovery.

11.5. **Application Vulnerability Assessment.** We will perform an application security vulnerability assessment prior to any new public release. We will have a defined process to address any findings and will ensure that any high-risk vulnerabilities are addressed within 30 days of discovery.

11.6. **Penetration Tests and Security Evaluations of Websites.** We will perform a comprehensive penetration test and security evaluation of all systems and websites involved in providing Software on a recurring basis no less frequently than once annually. Additionally, we will have an industry-recognized independent third party perform an annual test. We will have a defined process to address any findings but will ensure that any high-risk vulnerabilities are addressed within 30 days of discovery. Upon Client's written request, but no more than once per year, we will provide an assertion statement to validate the completion of the independent third-party penetration test and attest to the fact that we maintain a process to address findings.

12. GLIFFY RELATIONSHIPS

12.1. If we use a third-party application or service to provide the Software, our contract with that third-party vendor must clearly outline security requirements for the third-party vendor consistent with the security requirements of these Security Terms. In addition, we will ensure clearly defined service level agreements with the third party are in place.

12.2. Any third-party gaining access to our systems must be covered by a signed agreement containing confidentiality and security provisions consistent with the confidentiality and security requirements of the Agreement and these Security Terms.

12.3. We will perform quality control and security management oversight of outsourced software development.

13. INFORMATION SECURITY BREACH MANAGEMENT

13.1. Security Breach Response Process

13.1.1. We will maintain a record of Security Breaches noting the description of the Security Breach, the applicable time periods, the impact, the person reporting it, to whom the Security Breach was reported, and the actions taken to remediate the Security Breach.

13.1.2. If there is a Security Breach, we will:

13.1.2.1. notify Client of the Security Breach by contacting Client's point of contact in writing promptly, and in any event within 72 hours following the discovery of the Security Breach;

13.1.2.2. promptly investigate the Security Breach;

13.1.2.3. promptly provide Client with all relevant detailed information about the Security Breach; and

13.1.2.4. take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Breach. All Security Breach information we provide to Client is Confidential Information.

14. SECURITY COMPLIANCE AND ASSESSMENT

14.1. Gliffy maintains several security certifications such as SOC 2 and ISO 42001.

14.2. We operate an enterprise security management system aligned with ISO-based management system principles

and validated through ISO and SOC 2 independent assessments. This program establishes standardized policies, roles, and risk management processes, and ensures that security controls are consistently designed, implemented, monitored, and improved across our environment.

- 14.3. **Client Security Assessment.** Upon Client's reasonable request, but no more than once annually, we will complete, in a timely and accurate manner, an information security questionnaire Client provides to verify our compliance with these Security Terms ("**Security Assessment**"). For organizations utilizing more than one Gliffy Product, Client may audit one product per calendar year or may annually submit a consolidated questionnaire to cover all utilized products. If after completion of the Security Assessment, Client reasonably determines, or in good faith believes, that our security practices and procedures do not meet our obligations under the Agreement or these Security Terms, then Client will notify us of the perceived deficiencies. We will evaluate such perceived deficiencies and engage Client (as necessary) to determine if such deficiencies are actual deficiencies in our security practices and procedures.