

SS&C|Blue Prism Terms of Use Addendum for Subscription Services: Security Addendum

This SS&C|Blue Prism Security Addendum (this “**Security Addendum**”) forms part of your Agreement for the Subscription Services named in your Order and contains additional terms applicable to such Subscription Services. Capitalized terms used but not defined in this Security Addendum have the meanings ascribed to them in the Terms of Use Addendum for Subscription Services, General Terms or your Order, as applicable.

1. **Security Program.** We will maintain a comprehensive, commercially reasonable information security program under which we document, implement and maintain the physical, administrative, and technical safeguards reasonably designed and implemented to: (i) comply with laws applicable to our business; and (ii) protect against unauthorized access to, or disclosure of, Customer Data, such as unauthorized access or disclosure is referred to as a “**Security Incident**”. Such safeguards shall be consistent with industry standard security frameworks.
2. **Policies and Procedures.** We will maintain written information security management policies and procedures (configured in accordance with our security program) reasonably designed and implemented to identify, prevent, detect, contain, and correct violations of measures taken to protect the security of Customer Data. Such policies and procedures will, at a minimum:
 - a. assign specific data security responsibilities and accountabilities to specific individual(s);
 - b. describe acceptable use of our assets, including computing systems, networks, and messaging;
 - c. provide authentication rules for the format, content and usage of passwords for end users, administrators, and systems;
 - d. describe logging and monitoring of production environments, including logging and monitoring of physical and logical access to networks and systems that process or store Customer Data;
 - e. include an incident response process;
 - f. enforce commercially reasonable practices for user authentication;
 - g. include a formal risk management program which includes periodic risk assessments; and
 - h. provide an adequate framework of controls reasonably designed to safeguard Customer Data.
3. **Access control.** In connection with your use of the Subscription Services, you acknowledge you may connect the Subscription Services to your systems, applications, and software for you to process Customer Data, you are in control of access to Customer Data, and we are only able to access Customer Data if you grant us such access. You may grant us access to Customer Data through your configuration of the Subscription Services. In accordance with such configuration, we may have access to, receive, handle, store, or otherwise process Customer Data. Recommended best practices with respect to configuration of the Subscription Services are as set forth in the Documentation, and if you configure, or request us to make any configuration inconsistent with our recommended best practices, you relieve us of any liability arising out of such configuration. In any event, you shall comply with data minimization principles in deciding whether to grant us access to Customer Data or to provide Customer Data to us, and except for limited personal data such as contact information to enable us to manage your account and to communicate with you, to the fullest extent possible, you shall only provide us with access to technical data or data that is anonymized, pseudonymized, or “dummy data”, so it is not feasible for us to reasonably re-identify any actual individuals from such data.
4. **IT Change and Configuration Management.** We shall employ our own reasonable processes, for change management, code inspection, repeatable builds, separation of development and production environments, and testing plans. Code inspections will include a comprehensive process reasonably designed and implemented to identify vulnerabilities and malicious code. In addition, we will ensure that processes are implemented for purposes of vulnerability management, patching, and verification of system security controls prior to their connection to production networks.
5. **Certification Testing.** Following your written request, and no more than per calendar year, we will provide you with a current copy of any relevant security certification(s) and a summary of our periodic pen tests. We will take steps to resolve material vulnerabilities identified by such pen tests. If any patches or updates are required to remediate vulnerabilities, it is your responsibility to implement such patches and updates in a timely manner to prevent vulnerabilities.
6. **Personnel.** All personnel who have access to Customer Data are subject to background checks, confidentiality obligations and receive security and data privacy awareness training appropriate to their job function in accordance with industry standards.
7. **Monitoring and logging.** We will gather and analyze information regarding new and existing threats and vulnerabilities (such as multiple log-in attempts and log-ins from different locations), actual attacks on the Subscription Services, and the effectiveness of existing Subscription Services security controls. We log, and enable you to log within the Subscription Services, access and use of systems processing Customer Data.
8. **Security Incidents.** We will promptly notify you if we confirm any Security Incident within any specific time period required under laws applicable to us. In the event of a Security Incident, we will cooperate with you to investigate such Security Incident, as reasonably required, promptly undertake appropriate remediation measures (as reasonably determined by us in accordance with our policies, procedures and industry standards) with respect to your subscription to the Subscription Services, and we will provide updates to you of such remediation efforts. It is your responsibility to determine how, whether, when to provide notice of a Security Incident in accordance with the laws that are applicable to you.
9. **Encryption.** We have a policy that describes our encryption standards, method and strength used to protect or enable Customer to protect Customer Data (including authentication credentials) within the Subscription Services. Customer Data shall be encrypted consistent with industry standards at rest and while in transit over any public shared network and non-wired network. See the Documentation for further details about the relevant encryption method(s).
10. **Physical and environmental security.** We shall: (i) have measures in place to restrict entry to our offices where Customer Data is processed solely to authorized individuals; and (ii) ensure commercially reasonable practices are in place for infrastructure systems, including fire extinguishing, cooling and back-up power supply.
11. **Data Destruction.** Customer Data is retained as set forth in the Documentation and in accordance with your configuration of the Subscription Services. You may request to delete or destroy Customer Data within the Subscription Services prior to termination or expiration of your subscription to the Subscription Services in accordance with the Agreement. We will inform you if such deletion of Customer Data will impact the performance or functionality of the Subscription Services, and you agree to assume any risk in connection with the deletion or destruction of Customer Data. Any Customer Data remaining in the Subscription Services is deleted ninety (90) days following termination or expiration of your subscription to the Subscription Services.
12. **Term.** This Security Addendum remains in effect for the Term of your Order and automatically terminates thereafter. Our security policies, procedures and program are subject to change at any time in our sole discretion provided that such changes do not materially degrade the controls in comparison with those provided by us at the time we agreed to this Security Addendum.