SECURITY & PRIVACY DOCUMENTATION

(last updated May 21, 2018)

Olono's Commitment to Security & Privacy

Olono is committed to achieving and preserving the trust of our customers, by providing a comprehensive security and privacy program that carefully considers data protection matters across our suite of products and services, including data submitted by customers to our online service ("Customer Data").

Covered Services

This documentation describes the security-related and privacy-related audits and certifications received for, and the administrative, technical, and physical controls applicable to, the Olono online services branded as "Olono Actions", "Productivity Boost", "Process Effectiveness", "Pipeline Management", (collectively, the "Service"). This documentation does not apply to free trial services made available by Olono.

Architecture, Data Segregation, and Data Processing

The Service is operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The Olono architecture provides an effective logical data separation for different customers via customer-specific "Team IDs" and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, such as for testing and production.

Olono has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by Olono and its sub-processors.

Security Controls

The Service includes a variety of configurable security controls that allow Olono customers to tailor the security of the Service for their own use. Olono personnel will not set a defined password for a user. Each customer's users are provided with a token that they can use to set their own. Olono strongly encourages all customers, where applicable in their configuration of the Service's security settings, to use the single sign on features made available by Olono.

Information Security Management Program ("ISMP")

Olono maintains a comprehensive information security management program that contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of Olono's business; (b) the amount of resources available to Olono; (c) the type of information that Olono will store and process; and (d) the need for security and protection from unauthorized disclosure of such Customer Data. The ISMP is documented and updated based on changes in legal and regulatory requirements related to privacy and data security practices and industry standards applicable to the Service.

Olono's ISMP is designed to:

. Protect the integrity, availability, and prevent the unauthorized disclosure by Olono or its agents, of Customer Data in Olono's possession or control;

. Protect against any anticipated threats or hazards to the integrity, and availability, and prevention of unauthorized disclosure of Customer Data by Olono or its agents;

. Protect against unauthorized access, use, alteration, or destruction of Customer Data;

. Protect against accidental loss or destruction of, or damage to, Customer Data; and

. Safeguard information as set forth in any local, state or federal regulations by which Olono may be regulated.

1. **Security Standards.** Olono's ISMP includes adherence to and regular testing of the key controls, systems and procedures of its ISMP to validate that they are properly implemented and effective in addressing the threats and risks identified. Such testing includes:

a) Internal risk assessments;

b) SSAE18 SOC1 Type 1 and SOC2 Type I (or successor standard) audits in progress by accredited third-party auditors ("Audit Report").

2. **Security Audit Report.** Olono provides its customers, upon their request, with a copy of Olono's then-current Audit Report, including information as to whether the Security Audit revealed any material findings in the Service; and if so, the nature of each finding discovered.

3. **Assigned Security Responsibility.** Olono assigns responsibility for the development, implementation, and maintenance of its Information Security Management Program, including:

a) Designating a security official with overall responsibility;

and

b) Defining security roles and responsibilities for individuals with security responsibilities.

4. **Relationship with Sub-processors.** Olono conducts reasonable due diligence and security assessments of sub- processors engaged by Olono in the storing and/or processing of Customer Data ("Sub-processors"), and enters into agreements with Sub-processors that contain provisions similar or more stringent than those provided for in this security and privacy documentation.

5. **Background Check**. Olono performs background checks on any employees who are to perform material aspects of the Service or have access to Customer Data.

6. **Security Policy, Confidentiality.** Olono requires all personnel to acknowledge in writing, at the time of hire, that they will comply with the confidential data identification and protection policy and protect all Customer Data at all times.

7. **Security Awareness and Training.** Olono has mandatory security awareness and training programs for all Olono personnel that address their implementation of and compliance with the ISMP.

8. **Disciplinary Policy and Process**. Olono maintains a disciplinary policy and process in the event Olono personnel violate the ISMP.

9. **Access Controls.** Olono has in place policies, procedures, and logical controls that are designed:

a) To limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons;

b) To prevent personnel and others who should not have access from obtaining access; and

c) To remove access in a timely basis in the event of a change in job responsibilities or job status.

Olono institutes:

. Controls to ensure that only those Olono personnel with an actual need-to-know will have access to any Customer Data;

. Controls to ensure that all Olono personnel who are granted access to any Customer Data are based on least-privilege principles;

. Periodic (no less than quarterly) access reviews to ensure that only those Olono personnel with access to Customer Data still require it.

12. Data Encryption.

. a) Encryption of Transmitted Data: Olono uses Internet-industry-standard secure encryption methods designed to encrypt communications between its server(s) and the customer browser(s), and between its servers and customer's server(s).

. b) Encryption of At-Rest Data: Olono uses Internet-industry standard secure encryption methods designed to protect stored Customer Data at rest. Such information is stored on server(s) that are not accessible from the Internet.

. c) Encryption of Backups: All offsite backups are encrypted. Olono uses disk storage that is encrypted at rest.

13. Disaster Recovery. Olono maintains policies and procedures for responding to an emergency or a force majeure event that could damage Customer Data or production systems that contain Customer Data. Such procedures include:

a) Data Backups: A policy for performing periodic backups of production file systems and databases to meet the Recovery Point Objective described below;

b) Disaster Recovery: A formal disaster recovery plan for the production environment designed to minimize disruption to the Service, which includes requirements for the disaster plan to be tested on a regular basis, currently daily;

c) Business Continuity Plan: A formal process to address the framework by which an unplanned event might be managed in order to minimize the loss of vital resources.

14. Secure Development Practices. Olono adheres to the following development controls:

a) Development Policies: Olono follows secure application development policies, procedures, and standards that are aligned to industry-standard practices, such as the OWASP Top 10 and SANS Top 20 Critical Security Controls; and

b) Training: Olono provides employees responsible for secure application design, development, configuration, testing, and deployment appropriate (based on role) training by the security team

regarding Olono's secure application development practices.

15. Malware Control. Olono employs then-current industry-standard measures to test the Service to detect and remediate viruses, Trojan horses, worms, logic bombs, or other harmful code or programs designed to negatively impact the operation or performance of the Service.

16. Data Integrity and Management. Olono maintains policies that ensure the following:

a) Segregation of Data: The Service includes logical controls, including encryption, to segregate each customer's Customer Data from that of other customers; and

b) Back Up/Archival: Olono performs full backups of the database(s) containing Customer Data no less than once per day and archival storage on no less than a weekly basis on secure server(s) or on other commercially acceptable secure media.

17. Vulnerability Management. Olono maintains security measures to monitor the network and production systems, including error logs on servers, disks and security events for any potential problems. Such measures include:

a) Infrastructure Scans: Olono performs quarterly vulnerability scans on all infrastructure components of its production and development environment. Vulnerabilities are remediated on a risk basis. Olono installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible;

b) Application Scans: Olono performs quarterly (as well as after making any major feature change or architectural modification to the Service) application vulnerability scans. Vulnerabilities are remediated on a risk basis. Olono installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible;

c) External Application Vulnerability Assessment: Olono engages third parties to perform network vulnerability assessments and penetration testing on an quarterly basis ("Vulnerability Assessment"). Reports from Olono's then-current Vulnerability Assessment, together with any applicable remediation plans, will be made available to customers on written request.

Vulnerabilities are remediated on a risk basis. Olono installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible.

18. Change and Configuration Management. Olono maintains policies and procedures for managing changes to production systems, applications, and databases. Such policies and procedures include:

a) A process for documenting, testing and approving the promotion of changes into production;

b) A security patching process that requires patching systems in a timely manner based on a risk analysis; and

c) A process for Olono to perform security assessments of changes into production.

19. Intrusion Detection. Olono monitors the Service generally for unauthorized intrusions using traffic and activity-based monitoring systems. Olono may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to help customers detect fraudulent authentications, and to ensure that the Service functions properly.

20. Incident Management. Olono has in place a security incident response plan that includes procedures to be followed in the event of any unauthorized disclosure of Customer Data by Olono or its agents of which Olono becomes aware to the extent permitted by law (such unauthorized disclosure defined herein as a "Security Breach"). The procedures in Olono's security incident response plan include:

a) Roles and responsibilities: formation of an internal incident response team with a response leader;

b) Investigation: assessing the risk the incident poses and determining who may be affected;

c) Communication: internal reporting as well as a notification process in the event of a Security Breach;

d) Recordkeeping: keeping a record of what was done and by whom to help in subsequent analyses; and

e) Audit: conducting and documenting a root cause analysis and remediation plan.

Olono publishes system status information on the Olono Trust website, at https://status.olono.ai. Olono typically notifies customers of significant system incidents by email to the listed admin contact, and for availability incidents lasting more than four hours , may invite impacted customers to join a conference call about the incident and Olono's response.

21. Security Breach Management.

a) Notification: In the event of a Security Breach, Olono notifies impacted customers of such Security Breach. Olono cooperates with an impacted customer's reasonable request for

information regarding such Security Breach, and Olono provides regular updates on any such Security Breach and the investigative action and corrective action(s) taken.

b) Remediation: In the event of a Security Breach, Olono, at its own expense, (i) investigates the actual or suspected Security Breach, (ii) provides any affected customer with a remediation plan, to address the Security Breach and to mitigate the incident and reasonably prevent any further incidents, (iii) remediates the effects of the Security Breach in accordance with such remediation plan, and (iv) reasonably cooperates with any affected customer and any law enforcement or regulatory official investigating such Security Breach.

22. Logs. Olono provides procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports. (i) implements commercially reasonable measures to protect such logs from unauthorized modification or erasure, and (ii) retains such logs in compliance with Olono's data retention policy. If there is suspicion of inappropriate access to the Service, Olono has the ability to provide customers log entry records to assist in forensic analysis. This service will be provided to customers on a time and materials basis.