CRESTA ENTERPRISE SECURITY ADDENDUM

This Enterprise Security Addendum (ESA) outlines the security measures that Cresta Intelligence Inc. ("Cresta") implements to safeguard all Customer Content processed within the Cresta Platform and is incorporated into the Agreement by reference. Capitalized terms not defined in this ESA shall have the meanings ascribed to them in the Agreement. In the event of any conflict or inconsistency between this ESA and the Agreement, this ESA will control respect to the subject matter herein. For detailed documentation and relevant certifications associated with each measure, please visit the Cresta Trust Center.

1. Security Leadership and Organization

Cresta has a dedicated security team led by Cresta's Head of Security, Compliance & IT, who reports directly to the CEO and is chartered to define, supervise implementation of, and monitor all relevant security policies, standards, and controls (the "Security Team"). The Security Team maintains independence from Cresta's development and engineering teams to ensure objective oversight. Regular validation of security controls and reporting to leadership empowers informed decision-making for continuous security improvement. Additionally, Cresta's Security Team, along with independent auditors, provide comprehensive security posture and internal control assessments.

2. Independent Audits and Verifications

Cresta undergoes annual independent security audits based on risk assessments and established policies. Cresta maintains reports such as SOC 2 Type II and certifications such as ISO 27001:2022, ISO 27701:2019, ISO 42001:2023 and PCI-DSS (or a similar industry standard). Cresta shall make available to Customer information necessary to demonstrate compliance with this ESA and shall reasonably contribute to assessments by Customer.

3. Regular Security Risk Assessments

Cresta conducts annual information security risk assessments. These assessments may also occur more frequently in response to significant changes in Cresta's business practices or technology that could impact privacy, confidentiality, security, integrity, or availability of Customer Content. These assessments, which include verification of administrative, procedural, and technical controls, are performed by qualified third-party assessors, penetration testers, or Cresta's Security Team. Any critical findings are addressed and tracked to completion.

4. Incident Response

Cresta maintains an Incident Response Plan ("IRP") managed by the Security Team. This plan is reviewed and tested annually. Security incidents are assigned a severity level, investigated, and resolved. Post-incident reviews are conducted for severe incidents. The IRP defines response times based on severity, outlines roles and responsibilities, and establishes incident declaration procedures. Depending on the severity, the Security Team and other relevant stakeholders will continuously monitor issues and communicate with customers as needed, following the notification provisions of the Agreement.

5. Secure Configuration Management

Cresta leverages industry-standard security baselines and vendor best practices to ensure appropriate secure configuration of its production environments. Unused services are disabled and blocked. Configurations are reviewed and updated periodically by operations staff and the Security Team.

6. Application Security and Vulnerability Management

Cresta upholds a rigorous security testing and vulnerability management program. Annual application penetration testing and infrastructure red team testing are conducted by external parties. Identified vulnerabilities are remediated according to Cresta's vulnerability management policy, with the following timelines for resolution based on severity:

Rating	**Resolution Timeframe**
Critical	7 days
High	14 days
Medium	60 days
Low	90 days
Informational	Backlog

Cresta adheres to a Secure Development Lifecycle ("SDL") process aligned with industry standards and best practices. This risk-based approach incorporates periodic static testing, dynamic testing, and other techniques to identify security vulnerabilities in major code releases. The Security Team manages these identified issues. Developers receive secure code training incorporating OWASP Top 10 guidelines. Source code management and deployment follow segregation of duties and least privilege principles. Separate environments are maintained for development, testing, QA, and production. Production data is not stored or used in testing environments. Tools or techniques used to assess security or attack systems without Cresta's authorization (e.g., vulnerability scanners, port scanners, penetration tools) are strictly prohibited.

7. Personnel Security and Training

Cresta requires thorough background checks for all employees before they begin their employment. The background checks, compliant with applicable law, may assess criminal history, employment verification, education verification, social security verification, national sex offender registry checks, global sanctions and enforcement checks, and physical address verification. Additionally, employees undergo mandatory security awareness training upon hire and annually thereafter.

8. Data and System Recovery

Cresta's production systems and services are designed to achieve a Recovery Time Objective (RTO) of 4 hours and a Recovery Point Objective (RPO) of 4 hours. The associated processes are regularly reviewed and tested.

9. Device Security

Cresta operates as a cloud-based service, ensuring that Customer Content resides within isolated cloud instances. Storing Customer Content on employee devices is strictly prohibited. Cresta centrally manages and pre-configures employee laptops. This pre-configuration incorporates the following security measures:

- Endpoint Detection and Response (EDR) and Antivirus Agent
- Full Disk Encryption
- No USB Access
- Inactivity Logout Enforcement
- Minimum 15 Character Password Requirement
- Firewall Protection
- Revoked Administrative Rights

Furthermore, only Cresta-issued laptops are authorized to connect to Cresta's backend systems.

10. Security Controls

10.1. Safeguarding Physical and Network Environments

Cresta leverages the capabilities of its public cloud provider to implement and maintain robust physical access controls. These controls protect servers, networks, and facilities from unauthorized access. Examples include:

- Secure buildings with multiple secure access zones
- Secure perimeters
- 24/7 video surveillance
- On-site security personnel
- Environmentally controlled data centers with uninterruptible power supplies
- Additional services mandated by relevant regulations

Cresta periodically validates the effectiveness of these controls through third-party security audits and vendor assessments. For a list of Cresta's cloud providers, please refer to the subprocessor list available at https://trust.cresta.com/.

10.2. Logical Access and Data Transmission Security

Logical access to Cresta's servers is restricted to authorized Cresta IT personnel with a demonstrable need. The Cresta Platform resides behind a jointly managed perimeter security system implemented by Cresta and its cloud

provider. This design prevents unauthorized direct communication sessions originating from the internet from reaching the internal network. Cresta continuously monitors its servers for any signs of unusual access activity.

Industry-standard security controls are in place to safeguard all Customer Content in transit. These controls include the use of appropriate network protocols, encryption schemes, data hashing, cryptographic signatures, and secure management practices for cryptographic keys and other secrets.

10.3. Data Storage and Access Controls

All media containing Customer Content is protected against unauthorized physical access. Customer Content at rest is encrypted using current and industry-standard encryption mechanisms. Cresta adheres to industry best practices for cryptographic key management. Cresta's third-party cloud hosting providers utilize NIST SP800-88 data destruction techniques to ensure Customer Content is unrecoverable upon deletion.

Cresta implements industry-standard identity governance processes and authentication mechanisms to restrict system access to authorized users only. This includes multi-factor authentication, single sign-on architecture (where feasible), device trust, and timely user provisioning and deprovisioning procedures. All user actions, including successful and failed login attempts, timestamps, IP addresses, and usernames, are logged. To securely authenticate into the Cresta platform, all customers are required to either integrate their SSO solution with their Cresta instance or leverage Cresta's two-factor authentication capabilities for all user accounts.

Following the principle of least privilege, access to specific data, systems, or services is limited to authorized users with a need-to-know basis. Role-based access control is implemented wherever possible, along with periodic access recertifications.

Remote access to Cresta's backend systems is restricted to authorized personnel based on their roles. This access adheres to the principle of least privilege and a multi-tiered security protocol encompassing IAM roles, single sign-on, two-factor authentication, VPN, and device trust.

10.4. Communication and Processing Controls

Cresta verifies and establishes the identities of parties to whom personal data may be transmitted or otherwise made available. Subprocessors used by Cresta undergo regular assessments to ensure their data security and privacy practices align with Cresta's own standards.

Cresta implements limitations, monitoring, and logging (where applicable) on how data is entered into its systems. Standard software development security controls are in place to sanitize potentially harmful external input. These controls include industry-standard measures designed to prevent the introduction or spread of malware.

All processing activities conducted by Cresta are performed on behalf of and at the direction of Customer. Processes and technical controls in place to enforce this are subject to periodic reviews.

10.5. Availability Controls

Multiple controls safeguard all data critical to Cresta Platform operations, including Customer Content. These controls ensure continuous data protection and include measures like utilizing multiple availability zones and adhering to other relevant industry-standard controls.