**Cresta Intelligence, Inc.**
**Data Processing Agreement**
(Updated May 2023)

This **Data Processing Agreement ("DPA")** is entered into as of the Effective Date (as defined in the Agreement), by Cresta Intelligence, Inc. ("Cresta") and the party entering into the Agreement with Cresta that refers to this DPA (the "Customer"). This DPA shall be deemed a part of the Agreement between Cresta and Customer governing the contractual relationship between Cresta and Customer, regardless of whether this document is signed. In the event of a conflict between the terms and conditions of this DPA and the Agreement, the terms and conditions of this DPA shall take precedence. All capitalized terms used in this Addendum and not defined in this Addendum shall have the meanings given to them in the Agreement.

1. Definitions

For this DPA, the terms below have the meanings set forth below. Capitalized terms used but not defined in this DPA have the meanings in the Agreement.

(a) Affiliate means any entity that directly or indirectly controls, is controlled by, or is under common control with the entity, where "control" refers to the power to direct or cause the direction of the entity, whether through ownership of voting securities, by contract or otherwise.

(b) Applicable Data Protection Laws means the privacy, data protection and data security laws and regulations of any jurisdiction applicable to the Processing of Personal Data under the Agreement, including, without limitation, European Data Protection Laws and the CCPA.

(c) CCPA means the California Consumer Privacy Act of 2018 and any regulations promulgated.

(d) CPRA means the California Privacy Rights Act of 2020 and any regulations promulgated.

(e) EEA means the European Economic Area.

(f) European Data Protection Laws means the GDPR and other data protection laws and regulations of the European Union, its Member States, Switzerland, Iceland, Liechtenstein, Norway and the United Kingdom, in each case, to the extent applicable to the Processing of Personal Data under the Agreement.

(g) GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as amended from time to time.

(h) Information Security Incident means a breach of Cresta's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Cresta's possession, custody or control. Information Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

(i) Personal Data means Customer Content that constitutes "personal data," "personal information," or "personally identifiable information" defined in Applicable Data Protection Law, or information of a similar character regulated thereby, except that Personal Data does not include Usage Data or information pertaining to Customer's personnel or representatives who are business contacts of Cresta, where Cresta acts as a controller of such information.

(j) Processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(k) Security Measures has the meaning given in Section 4(a) (Cresta's Security Measures).

(l) Standard Contractual Clauses means the mandatory provisions of the standard contractual clauses for the transfer of personal data to processors established in third countries in the form set out by European Commission Decision 2010/87/EU.

(m) Subprocessors means third parties that Cresta engages to Process Personal Data in relation to the Services.

(n) Third Party Subprocessors has the meaning in Section 6 (Subprocessors).

(o) The terms controller, data subject, processor and supervisory authority as used in this DPA have the meanings in the GDPR.

2. Duration and Scope of DPA

(a) This DPA will remain in effect if Cresta Processes Personal Data, notwithstanding the expiration or termination of the Agreement.

(b) Annex 1 (EU Annex) to this DPA applies solely to Processing subject to European Data Protection Laws. Annex 2 (California Annex) to this DPA applies solely to Processing subject to the CCPA if Customer is a "business" or "service Cresta" (as defined in CCPA) regarding such Processing.

3. Customer Instructions

Cresta will Process Personal Data only under Customer's instructions to Cresta. This DPA is a complete expression of such instructions, and Customer's additional instructions will bind Cresta only under an amendment to this DPA signed by both parties. Customer instructs Cresta to Process Personal Data to provide the Services as contemplated by this Agreement.

4. Security

(a) Cresta Security Measures. Cresta will implement and maintain technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data (the "Security Measures") as described in Annex 3 (Security Measures). Cresta may update the Security Measures from time to time, so long as the updated measures do not decrease the overall protection of Personal Data.

(b) Security Compliance by Cresta Staff. Cresta will ensure that its personnel authorized to access Personal Data are subject to appropriate confidentiality obligations.

(c) Cresta Security Assistance. Cresta will (considering the nature of the Processing of Personal Data and the information available to Cresta) provide Customer with reasonable assistance for Customer to comply with its obligations regarding Personal Data under Applicable Data Protection Laws, including Articles 32 to 34 (inclusive) of the GDPR where applicable, by (a) implementing and maintaining the Security Measures; and (b) complying with the terms of Section 4(d) (Information Security Incidents) of this DPA.

(d) Information Security Incidents. Cresta will notify Customer within 72 hours of learning of an Information Security Incident. Such notifications will describe available details of the Information Security Incident, including steps taken to mitigate the potential risks and steps Cresta recommends Customer take to address the Information Security Incident. Cresta's notification of or response to an Information Security Incident will not be construed as Cresta's acknowledgement of any fault or liability regarding the Information Security Incident.

(e) Customer's Security Responsibilities and Assessment

(i) Customer's Security Responsibilities. Customer agrees that, without limitation of Cresta's obligations under Section 4 (Security), Customer is solely responsible for its use of the Services, including (a) appropriately using the Services to ensure a level of security appropriate to the risk regarding the Personal Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Services; (c) securing Customer's systems and devices that Cresta uses to provide the Services; and (d) backing up Personal Data.

(ii) Customer's Security Assessment. Customer agrees that the Services, the Security Measures and Cresta's commitments under this DPA are adequate to meet Customer's needs, including regarding any security obligations of Customer under Applicable Data Protection Laws, and provide a level of security appropriate to the risk regarding the Personal Data.

(f) Data Deletion. Cresta shall delete all the Personal Data on Cresta's systems on Customer's request and after the end of the provision of Services and shall delete existing copies unless continued storage of the Personal Data is required by (i) applicable laws of the European Union or its Member States, regarding Personal Data subject to European Data Protection Laws or (ii) Applicable Data Protection Laws, regarding all other Personal Data. Cresta will comply with such instruction when reasonably practicable and within 180 days after such expiration or termination, unless Applicable Data Protection Laws require storage. Customer may request a copy of such Personal Data from Cresta for an additional charge by requesting it in writing at least 30 days before expiration or termination of the Agreement. Upon the parties' agreement to such charge under a statement of work or other amendment to the Agreement, Cresta will provide such copy of such Personal Data before it is deleted under this clause.

5. Data Subject Rights

(a) Cresta's Data Subject Request Assistance. Cresta will (considering the nature of the Processing of Personal Data) provide Customer with assistance reasonably necessary for Customer to perform its obligations under Applicable Data Protection Laws to fulfill requests by data subjects to exercise their rights under Applicable Data Protection Laws ("Data Subject Requests") with respect to Personal Data in Cresta's possession or control. Customer shall compensate Cresta for any such assistance at Cresta's then-current professional services rates, which shall be provided to Customer upon request.

(b) Customer's Responsibility for Requests. If Cresta receives a Data Subject Request, Cresta will advise the data subject to submit the request to Customer and Customer will be responsible for responding to the request.

6. Subprocessors

(a) Consent to Subprocessor Engagement. Customer authorizes the engagement of Subprocessors ("Third Party Subprocessors").

(b) Requirements for Subprocessor Engagement. When engaging any Subprocessor, Cresta will contract with such Subprocessor containing data protection obligations not less protective than those in this DPA regarding Personal Data to the extent applicable to the nature of the services provided by such Subprocessor. Cresta shall be liable for all obligations under the Agreement subcontracted to the Subprocessor and its actions and omissions related thereto.

7. Reviews and Audits of Compliance

Customer may audit Cresta's compliance with its obligations under this DPA up to once per year and on such other occasions as required by Applicable Data Protection Laws, including where mandated by Customer's supervisory authority. Cresta will contribute to such audits by providing Customer or Customer's supervisory authority with the information and assistance reasonably necessary to conduct the audit. If a third party is to conduct the audit, Cresta may object to the auditor if the auditor is, in Cresta's reasonable opinion, not independent, a competitor of Cresta, or otherwise manifestly unsuitable. Such objection by Cresta will require Customer to appoint another auditor or conduct the audit itself. To request an audit, Customer must submit a proposed audit plan to Cresta at least two weeks before the proposed audit date and any third party auditor must sign a customary non-disclosure agreement mutually acceptable to the parties (such acceptance not to be unreasonably withheld) providing for the confidential treatment of all information exchanged with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Cresta will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Cresta security, privacy, employment or other relevant policies). Cresta will work cooperatively with Customer to agree on a final audit plan. Nothing in this Section 7 shall require Cresta to breach any duties of confidentiality. If the controls or measures to be assessed in the requested audit are addressed in an SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third party auditor within twelve (12) months of Customer's audit request and Cresta has confirmed there have been no known material changes in the controls audited since the

date of such report, Customer agrees to accept such report in lieu of requesting an audit of such controls or measures. The audit must be conducted during regular business hours, subject to the agreed final audit plan and Cresta's safety, security or other relevant policies, and may not unreasonably interfere with Cresta business activities. Customer will promptly notify Cresta of any non-compliance discovered during an audit and provide Cresta any audit reports generated with any audit under this Section 7, unless prohibited by Applicable Data Protection Laws or otherwise instructed by a supervisory authority. Customer may use the audit reports only to meet Customer's regulatory audit requirements and/or confirming compliance with the requirements of this DPA. Any audits are at Customer's sole expense. Customer shall reimburse Cresta for any time expended by Cresta and any third parties with any audits or inspections under this Section 7 at Cresta's then-current professional services rates, which shall be provided to Customer upon request. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

8. Customer Responsibilities.

(a) Customer Compliance. Customer shall comply with its obligations under Applicable Data Protection Laws. Customer shall ensure (and is solely responsible for ensuring) that its instructions in Section 3 comply with Applicable Data Protection Laws, and that Customer has given all notices to, and has obtained all such from, individuals to whom Personal Data pertains and all other parties as required by laws or regulations for Customer to Process Personal Data as contemplated by the Agreement.

(b) Prohibited Data. Customer represents and warrants to Cresta that Customer Content does not and will not, without Cresta's prior written consent, contain any social security numbers or other government-issued identification numbers, protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA) or other information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; health insurance information; biometric information; passwords for online accounts; credentials to any financial accounts; tax return data; credit reports or consumer reports; any payment card information subject to the Payment Card Industry Data Security Standard; information subject to the Gramm-Leach-Bliley Act, Fair Credit Reporting Act or the regulations promulgated under either such law; information subject to restrictions under Applicable Data Protection Laws governing Personal Data of children, including, without limitation, all information about children under 13; or any information that falls within any special categories of data (as defined in GDPR).

9. Miscellaneous

Except as modified by this DPA, the terms of the Agreement remain in full force and effect. If any conflict occurs or inconsistency between this DPA and the other terms of the Agreement, this DPA will govern. Notwithstanding anything in the Agreement or any order form entered in connection therewith to the contrary, the parties acknowledge and agree that Cresta's access to Personal Data does not constitute part of the consideration exchanged by the parties regarding the Agreement. Notwithstanding anything to the contrary in the Agreement, any notices required or permitted to be given by Cresta to Customer under this DPA may be given (a) under any notice clause of the Agreement; (b) to Cresta's primary points of contact with Customer; or (c) to any email provided by Customer to provide it with Services-related communications or alerts. Customer is solely responsible for ensuring that such email addresses are valid.

*SIGNATURE PAGE FOLLOWS*

SIGNATURE PAGE TO DPA

IN WITNESS WHEREOF, the undersigned have executed this Agreement by their duly authorized representatives, intending to be legally bound.

| Customer: | Cresta: |
| --- | --- |
| **[INSERT]** | **CRESTA INTELLIGENCE, INC.** |
| By: _____ | By: _____ |
| Name: _____ | Name: _____ |
| Title: _____ | Title: _____ |

**ANNEX 1 TO DPA**

**EU ANNEX**

1. Processing of Data

   (a) Subject Matter and Details of Processing. The parties acknowledge and agree that (i) the subject matter of the Processing under the Agreement is Cresta's provision of the Services; (ii) the duration of the Processing is from Cresta's receipt of Personal Data until deletion of all Personal Data by Cresta under the Agreement; (iii) the nature and purpose of the Processing provides the Services; (iv) the data subjects to whom the Personal Data pertains are Customer's customers; and (v) the categories of personal data are data relating to Customer's customers, the extent of which is determined by Customer, such as contact information and communications.

   (b) Roles and Regulatory Compliance; Authorization. The parties acknowledge and agree that (i) Cresta is a processor of that Personal Data under European Data Protection Laws; (ii) Customer is a controller (or a processor acting on the instructions of a controller) of that Personal Data under European Data Protection Laws; and (iii) each party will comply with the obligations applicable to it in such role under the European Data Protection Laws regarding the Processing of that Personal Data. If Customer is a processor, Customer represents and warrants to Cresta that Customer's instructions and actions regarding Personal Data, including its appointment of Cresta as another processor, have been authorized by the relevant controller.

   (c) Cresta's Compliance with Instructions. Cresta will Process Personal Data only under Customer's instructions stated in this DPA unless European Data Protection Laws require otherwise, in which case Cresta will notify Customer (unless that law prohibits Cresta from doing so on important grounds of public interest).

2. Impact Assessments and Consultations

   Cresta will (considering the nature of the Processing and the information available to Cresta) reasonably assist Customer in complying with its obligations under Articles 35 and 36 of the GDPR, by (a) making available documentation describing relevant aspects of Cresta's information security program and the security measures applied in connection therewith and (b) providing the other information in the Agreement, including this DPA.

3. Data Transfers

   (a) Data Processing Facilities. Cresta may, subject to Section 3(b) (Transfers out of the EEA), store and Process Personal Data in the United States or anywhere Cresta or its Subprocessors maintains facilities.

   (b) Transfers out of the EEA. If Customer transfers Personal Data out of the EEA to Cresta in a country not deemed by the European Commission to have adequate data protection, such transfer will be governed by the Standard Contractual Clauses, the terms of which are incorporated into this DPA. In furtherance of the foregoing, the parties agree that

      (i) Customer will act as the data exporter and Cresta will act as the data importer under the Standard Contractual Clauses;

      (ii) for Appendix 1 to the Standard Contractual Clauses, the categories of data subjects, data, special categories of data (if appropriate), and the Processing operations shall be as set out in Section 1(a) to this Annex 1 (Subject Matter and Details of Processing);

      (iii) for Appendix 2 to the Standard Contractual Clauses, the technical and organizational measures shall be the Security Measures;

      (iv) data importer will provide the copies of the subprocessor agreements that must be sent by the data importer to the data exporter under Clause 5(j) of the Standard Contractual Clauses upon data exporter's request, and that data importer may remove or redact all commercial information or clauses unrelated the Standard Contractual Clauses or their equivalent beforehand;

(v) the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be performed under Section 7 (Reviews and Audits of Compliance) of the DPA;

(vi) Customer's authorizations in Section 6 (Subprocessors) of the DPA will constitute Customer's prior written consent to the subcontracting by Cresta of the Processing of Personal Data if such consent is required under Clause 5(h) of the Standard Contractual Clauses; and

(vii) certification of deletion of Personal Data as described in Clause 12(1) of the Standard Contractual Clauses shall be provided upon data importer's request.

Notwithstanding the foregoing, the Standard Contractual Clauses (or obligations the same as those under the Standard Contractual Clauses) will not apply to the extent an alternative recognized compliance standard for transferring Personal Data outside the EEA under European Data Protection Laws applies to the transfer. If any conflict occurs or inconsistency between (a) this Annex 1 and any other provision of this DPA, this Annex 1 will govern or (b) the Standard Contractual Clauses and any other provision of the Agreement, the Standard Contractual Clauses will govern.

## ANNEX 2 TO DPA

## CALIFORNIA ANNEX

1. For this Annex 2, the terms "business," "business purpose," "commercial purpose," "contractor," "sell" and "service provider" shall have the respective meanings given thereto in the CPRA, and "personal information" shall mean Personal Data that constitutes personal information governed by the CPRA.

2. It is the parties' intent that regarding any personal information, Cresta is a service provider and contractor, and Customer is a business. Cresta shall (a) not sell or share any personal information; (b) not retain, use or disclose personal information other than for the business purposes specified in the MSSA and DPA, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the MSSA and DPA, or as otherwise permitted by the CPRA; (c) not retain, use or disclose the personal information outside of the direct business relationship between Cresta and Customer; and (d) Combine the personal information that the Cresta receives pursuant to the MSSA and DPA with Customer with personal information that it receives from or on behalf of another person or persons, or collects from its own interaction with the consumer, provided that the Cresta may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) of Section 1798.140 and in regulations adopted by the California Privacy Protection Agency. Cresta certifies that it understands its obligations under this Section 2 and will comply with them.

3. The parties agree that (a) Personal information is disclosed by Customer only for limited and specified purposes set forth in the MSSA and DPA; (b) each party shall comply with applicable obligations under the CPRA and provide to consumers the same level of privacy protection as is required under the CPRA; (c) Cresta grants Customer the rights to take reasonable and appropriate steps to help ensure that Cresta uses the personal information transferred in a manner consistent with Customer's obligations under the CPRA; Cresta shall notify the Customer if it makes a determination that it can no longer meet its obligations under the CPRA; and (e) Cresta grants Customer the right, upon notice, including under subsection (d) of this paragraph, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

4. If Cresta engages any Subprocessors to assist it in processing personal information for a business purpose on behalf of the business, or if any Subprocessor engages another person to assist in processing personal information for that business purpose, it shall notify the Customer of that engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph 2 and 3 above.

5. The parties acknowledge that Cresta's retention, use and disclosure of personal information authorized by Customer's instructions documented in the MSSA and DPA are integral to Cresta's provision of the Services and the business relationship between the parties.

## ANNEX 3 TO DPA

## SECURITY MEASURES

1. Cresta has dedicated staff responsible for the development, implementation, and maintenance of Cresta's information security program. The Cresta Security and Compliance team comprises the Head of Security and Compliance and Governance Risk & Compliance Manager and works closely with Engineering Lead and Head of Infrastructure. The Security and Compliance team carries out all security policies and procedures. The team has a direct line to the CEO and can communicate with the CEO whenever they need to.

2. Cresta has audit and risk assessment procedures for periodic review and assessment of risks to Cresta. The Security and Compliance team carries out monitoring and maintaining compliance with Cresta's policies and procedures and reports the condition of its information security and compliance to internal senior management.

Cresta risk assessment methodology is based on *NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments*.

- Management defines the scope of risk assessment and creates the risk assessment team with a point person to guide the process (risk assessment project lead).
- If risk assessment procedures are not defined, the team should define them. The proper time and method of communicating the selected risk treatment options to the affected IT and business management should be included.
- Evaluate the system - Determine if the system is critical to the organization's business processes and determine the data classification and security needs of the data on the system according to the Cresta Data Classification Policy, considering security needs.
- List the threats - List possible threat sources such as an exploitation of a vulnerability.
- Identify vulnerabilities.
- Evaluate potential security controls already in place to assess if they adequately address the risk.
- Identify the probability of exploitation. Additional security controls may need to be in place before the probability of exploitation is lowered.
- Quantify damage (impact) - Categorize the damage and possibly place a dollar amount on the damage where possible. This will help when looking at cost of controls to reduce the risk.
- Determine risk level - Use likelihood times impact to quantify the amount of risk.
- Evaluate and recommend controls to reduce or eliminate risk - Identify existing controls and those that may further reduce probabilities or mitigate specific vulnerabilities. List specific threats and vulnerabilities for the system to help identify mitigating controls.
- Create an entry in Cresta's risk tracker.
- Communicate the selected risk treatment options to the affected IT and business management and staff.
- Take recommended risk mitigation actions. Record such actions as changes per the Cresta Change Management program.
- Monitor the effectiveness of the risk mitigation actions and document the results.

3. Cresta has strict data security controls which include, at a minimum, logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilization of commercially available industry-standard encryption technologies for Personal Data transmitted over public networks (i.e. the Internet) or when transmitted wirelessly or at rest or stored on portable or removable media (e.g. laptop computers). The Cresta application has a top-level NGINX load balancer only open on a single port. TLS is required for every connection to the Cresta application.

   For services within AWS, such as our Relational Database Service (RDS), we use AWS and GCP Key Management System (KMS) to encrypt customer data at rest via AES-256.

   Cresta's S3 buckets leverage Amazon's S3 server-side encryption which uses one of the strongest block ciphers available, AES-256.

4. Logical access controls designed to manage electronic access to data and system functionality based on job functions, (e.g. granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur). Cresta's employee access process is:

- Access requests for Cresta employees are made through our slack channel #it-requests.
- Access requests should be made to the Cresta employee or employees who manage the resource(s).
- Those employees will not grant access unless they are satisfied the additional access is necessary for the grantee to complete a necessary business task.
- When granting access, employees will ensure grants are scoped to the minimum breadth and duration to complete the business task. Root access will not be granted unless absolutely necessary to perform the job function.
- In addition, the employee(s) must accept the company's Acceptable Use Policy before access will be granted.

5. Password controls designed to manage and control password strength, expiration, and usage including prohibiting users from sharing passwords and requiring that Cresta's passwords that are assigned to its employees: (i) be at least eight (8) characters in length, (ii) not be stored in a readable format on Cresta's computer systems; (iii) must have defined complexity; (iv) must have a history threshold to prevent reuse of recent passwords; and (v) newly issued passwords must be changed after first use.

6. System audit and event logging proactively record all user access and system activity within our system architecture. Further, all business systems in scope also have audit logging enabled.

7. Physical and environmental security of areas containing Personal Data is designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor, and log the movement of persons into and out of the Cresta's facilities, and (iii) guard against environmental hazards such as heat, fire, and water damage.

8. Operational procedures and controls are in place for configuration, monitoring, and maintenance of technology and information systems, including secure disposal of systems and media to render all information or data contained as undecipherable or unrecoverable before final disposal or release from Cresta's possession. These procedures are covered in Cresta's Asset Management & Acceptable Use Policies.

9. Change management procedures and tracking mechanisms designed to test, approve, and monitor all material changes to Cresta's technology and information assets are covered in Cresta's Change Management Policy.

   All of Cresta's software is version controlled and synced between contributors (developers). Access to the central repository is restricted based on an employee's role.

   Using a decentralized version control system allows multiple developers to work simultaneously on features, bug fixes, and new releases; it also allows each developer to work on their own local code branches in a local environment.

   All code is written, tested, and saved in a local repository before being synced to the origin repository. Writing code locally decouples the developer from the production version of our code base and insulates us from accidental code changes that could affect our users. In addition, any changes involving the persistence layer (database) are performed locally when developing new code, where errors or bugs can be spotted before the change is deployed to users.

10. Incident response procedures are outlined in Cresta's Incident Response Policy and outline how Cresta investigates, responds to, mitigates, and notifies of events related to security and downtime incidents of Cresta's technology and information assets.

11. Vulnerability assessment, patch management and threat protection technologies, and scheduled monitoring procedures designed to identify, assess, mitigate, and protect against identified security threats, viruses, and other malicious code are defined in Cresta's Vulnerability Management Policy.

12. Business resiliency/continuity and disaster recovery procedures defined in Cresta's Disaster Recovery & Business Continuity Policies maintain service and/or recovery from foreseeable emergencies or disasters.