# Corelight Corporate Information Security Measures

These Corelight Corporate Information Security Measures ("**Security Measures**") set forth the administrative, physical and technical security measures that Corelight implements and maintains to protect: (a) Corelight's corporate network, applications and systems ("**Corporate Environment**") and (b) the security and confidentiality of any Customer Confidential Information contained therein.

Corelight's Cloud Products include their own security provisions as applicable. Please reference each Cloud Product's specific security measures for security information regarding such Cloud Product. These Security Measures do not apply to the security of Cloud Products.

Capitalized terms used and not defined in these Security Measures have the meanings given to them in the Corelight Customer Agreement located at www.corelight.com/legal/agreements (or such successor URL as may be designated by Corelight).

1. **SECURITY MANAGEMENT**.

   1.1. **Security Organization & Program**.

   (a) Corelight's chief information security officer ("**CISO**") leads Corelight's information security program and oversees a dedicated information security team. The CISO develops, reviews and approves (together with other internal stakeholders) Corelight's Security Policies (as defined below).

   (b) Corelight's information security program is reasonably designed to protect Corelight's Corporate Environment and the security, confidentiality, integrity and availability of Customer Confidential Information within Corelight's Corporate Environment. Corelight's information security program is intended to be appropriate to the size and complexity of Corelight's business and the type of information that Corelight's Corporate Environment stores.

   1.2. **Security Policies & Procedures**.

   (a) Corelight maintains information security, use and management policies (collectively, "**Security Policies**") designed to educate employees regarding their responsibilities with respect to Corelight's information security (including imposing disciplinary measures for failure to abide by such policies).

   (b) The Security Policies are evaluated and updated at least annually and are made available via the corporate intranet.

2. **PERSONNEL SECURITY & ONBOARDING**. All Corelight employees are subject to the following minimum security measures:

   2.1. **Screening**. All Corelight personnel undergo background checks prior to onboarding (as permitted by local law), which may include, but are not limited to, criminal record checks, employment history verification, education verification, and global sanctions and enforcement checks. Corelight uses a third-party provider to conduct screenings, which vary by jurisdiction and comply with applicable local law.

   2.2. **Confidentiality Agreements**. All Corelight personnel are required to sign non-disclosure/confidentiality agreements.

   2.3. **Training & Awareness**. Corelight personnel receive training on the Security Policies upon hire and refresher training annually. Employees are required to certify and agree to the Security Policies and personnel who violate the Security Policies are subject to disciplinary action, including warnings, suspension and up to (and including) termination. Corelight also conducts ongoing awareness of emerging security threats through various mechanisms, including simulated security-related incidents (e.g., phishing campaigns).

   2.4. **Controlled Access**. Corelight controls and limits access to its Corporate Environment and Customer Confidential Information (if applicable) strictly to authorized Corelight personnel only in accordance with Section 4 (Access Control).

3. **PHYSICAL & ENVIRONMENTAL CONTROLS**.

   3.1. **Corelight Corporate Offices**. Corelight has implemented administrative, physical and technical safeguards for its corporate offices. These include, but are not limited to: (a) requiring visitors to sign in, acknowledge and accept

an NDA, wear an identification badge and be escorted by Corelight personnel while on premises, (b) requiring Corelight employees to badge into the offices (badges cannot be shared or loaned to others without authorization), and (c) inventorying and tracking equipment and other Corelight-issued assets. Corelight partners with office building management to monitor physical entry points to office premises.

3.2. **Data Centers**. Corelight does not operate any of its own data centers. Corelight leverages third-party, industry-leading data center providers; these data center providers maintain extensive security controls, including secure design, access control, logging and monitoring, surveillance and detection, device management, and infrastructure maintenance. All data center providers are subject to the vendor management program outlined in Section 11.

4. **ACCESS CONTROL**.

4.1. **Provisioning Access**. Corelight follows the principles of least privilege when provisioning access and limits access to users who have a need to know. Corelight revokes an employee's access to systems and applications promptly upon termination of employment.

4.2. **Authentication**. Corelight personnel are authenticated through single sign-on (SSO) and use a unique user ID and password combination and multi-factor authentication.

4.3. **Password Controls**. Corelight's password management policy for Corelight personnel requires complexity, the use of longer character lengths and special characters.

5. **NETWORK SECURITY**.

5.1. **Network Architecture**. Corelight deploys firewall technology in the operation of Corelight's sites. Traffic between Corelight and customers will be protected and authenticated by industry standard cryptographic technologies (e.g., email transmissions are encrypted provided that the recipient supports TLS v1.2 connections).

5.2. **Intrusion Detection**. Corelight deploys an intrusion detection system to generate, monitor and respond to alerts which could indicate potential compromise of the network and/or host.

6. **ENDPOINT DEVICE SECURITY**.

6.1. **Workstations**. Corelight enforces certain security controls on Corelight-issued workstations used by personnel including: full disk encryption, anti-malware software, automatic patching configurations, screen lock with automatic activation features, and periodic scanning for restricted/prohibited software.

6.2. **Mobile Device Management**. Before connecting to a mobile device to corporate resources, Corelight personnel must enroll in Corelight's mobile device management ("**MDM**") application and meet MDM policy requirements (collectively, the "**MDM Program**"). Corelight's MDM Program enforces minimum security requirements, including monitoring, remote wiping capability, encryption and OS version updates.

7. **SECURE DEVELOPMENT**. Corelight applies security by design principles throughout the secure development lifecycle ("**SDLC**"). Corelight also applies the SDLC standard to perform numerous security-related activities for its software applications across different phases of the product creation lifecycle, from requirements gathering and product design all the way through product deployment. These activities include, but are not limited to, the performance of (a) internal security reviews before deploying new software or code, (b) open source security scans, (c) static and dynamic application security testing, (d) network vulnerability scans, and (e) external penetration testing. Corelight utilizes a code versioning control system to maintain the integrity and security of application source code. Access privileges to the source code repository are reviewed periodically and limited to authorized personnel. This change management program includes logically or physically separate environments from production for all development and testing.

8. **VULNERABILITY MANAGEMENT**. Corelight maintains controls and policies to mitigate the risk of security vulnerabilities in a measurable time frame that balances risk and the business and operational requirements.

8.1. **Monitoring & Detection**. Corelight monitors for vulnerabilities that are acknowledged by software vendors, reported by researchers or discovered internally. Corelight uses third-party tooling to conduct vulnerability scans regularly to assess vulnerabilities in its software applications and corporate systems. Periodically, Corelight engages independent, recognized third parties to conduct penetration tests.

8.2. **Verification & Mitigation**. Corelight verifies vulnerabilities, rates them according to industry-standard ratings systems, and identifies them for mitigation or fixes based on criticality level. Corelight leverages the National Vulnerability Database's Common Vulnerability Scoring System (CVSS), or where applicable, the U.S.-Cert rating, combined with an internal analysis of contextual risk to determine criticality. Confirmed vulnerabilities are remediated and/or mitigated in accordance with Corelight's internal criticality SLA matrix.

9. **STORAGE, HANDLING, DISPOSAL**.

9.1. **Data Segregation**. Corelight physically or logically separates and segregates Customer Confidential Information and Personal Data from its other customers' data.

9.2. **Encryption of Electronic Form Data**. Corelight utilizes strong industry standard encryption algorithms and key strengths (i.e., AES 256-bit at rest, TLS v1.2 in transit) to encrypt all Customer Confidential Information and Personal Data in electronic form while in transit over all public wired networks (e.g., Internet) and all wireless networks.

9.3. **Secure Disposal**. Customer Confidential Information and Personal Data is disposed of in a method that renders the data unrecoverable, to the extent reasonably possible, in accordance with industry best practices for wiping of electronic media (e.g., NIST SP 800-88).

10. **BREACH DETECTION & RESPONSE**.

10.1. **Detection**. Corelight maintains a security incident response team ("**SIRT**") to identify, report and appropriately respond to security incidents. The SIRT employs an incident response framework to manage and minimize the effects of unplanned security incidents. Customers may notify Corelight of suspected vulnerability or incident by submitting a technical support case for Corelight's evaluation.

10.2. **Security Breach**. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed Security Breaches, Corelight will take appropriate, reasonable steps to minimize unauthorized disclosure. "**Security Breach**" means any breach of Corelight's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data on systems managed by or otherwise controlled by Corelight. Security Breaches will 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, and other network attacks on firewalls or networked systems.

10.3. **Communications & Cooperation**. In the event of a Security Breach for which that Customer is impacted, Corelight will: (a) notify Customer in writing without undue delay after becoming aware of the Security Breach; and (b) promptly take reasonable steps to contain, investigate, and mitigate any adverse effects resulting from the Security Breach. Corelight will reasonably cooperate with and provide to Customer information in its possession to assist Customer in meeting Customer's obligations to report a Security Breach as required under applicable data protection laws, taking into account the nature of the processing, the information available to Corelight, and any restrictions on disclosing the information (such as confidentiality).

11. **THIRD PARTY VENDOR MANAGEMENT**. Corelight has implemented a vendor management program that applies the appropriate technical and organizational security controls that are proportional to the type of service the third-party vendor is providing and any associated security-related risks. Prospective third-party vendors are vetted through a process that ensures they comply with, and will continue to comply with, Corelight's confidentiality, security, and privacy requirements for the duration of their relationship with Corelight. Third-party vendors that process Customer Confidential Information are subject to more stringent technical and organizational security controls which are reflected in Corelight's contractual agreement with such third-party vendors. In addition, Corelight regularly reviews (a) each critical third-party vendor engaged against Corelight's security and business continuity standards; (b) each third-party vendor's access to Customer Confidential Information and its technical and organizational security controls to protect Customer Confidential Information; and (c) evolving legal or regulatory requirements that impact Corelight's security program or processing of Customer Confidential Information. Corelight's current third-party vendors that are sub-processors are available at www.corelight.com/legal/subprocessors.

12. **BUSINESS CONTINUITY & DISASTER RECOVERY**. Corelight identifies requirements for and implements a business continuity management program to prevent catastrophic data loss and ensure timely restoration of corporate

resources in the event of system failure, damage, or destruction. Corelight's business continuity and disaster recovery ("**BC/DR**") plans are established based on:

12.1. **Business Impact Analysis**. As part of its business impact analysis, Corelight conducts a systematic review of its Products, business functions and their associated dependencies, an evaluation of potential impact from disruptions, and defines business and technical recovery time objectives.

12.2. **Business Continuity Planning**. Corelight's business continuity planning addresses location, staffing, remote work strategies, and technology recovery steps.

12.3. **Disaster Recovery Planning**. Corelight's disaster recovery planning outlines infrastructure, technology, and system(s) details, recovery, and restoration activities, and identifies the people and technology teams required for such recovery.

Corelight ensures that its BC/DR plans address the actions and resources required to provide for (a) Corelight's continuous operation, and (b) in the event of an interruption, the recovery of the functions required to enable Corelight to provide the Products, including required systems, hardware, software, resources, personnel, and data supporting these functions.