cora

Security Policy

The Power of Perspective

Table of Contents

Security Policy

This Security Policy sets forth administrative, technical and physical safeguards Cora Systems (“Cora”) takes to protect customer data. Cora may update this Security Policy from time to time to reflect changes and improvements to our processes and technologies, as well as in response to emerging security threats.

Capitalized but undefined terms shall have the definitions given them in the Subscription Services Agreement (“SSA”).

The Framework

Cora has adopted a security model designed to comply with the following international best practice standards; ISO27001/ISO27002, SOC 2 Type 2, Cyber Essentials, and Cyber Essentials Plus.

The following are Cora’s key security objectives:

- Ensure that all data is held in a confidential state and only accessible to authorised users.
- Ensure that data integrity is maintained at all times.
- Ensure that data is available to the user when required.

Policies

Cora maintains security policies that are documented, approved, and periodically reviewed by management. These policies guide areas of security within Cora, covering the management of security for both Cora internal operations and the services Cora provides to its customers. Policies are communicated to all personnel including, where appropriate, contractors and third parties involved in the delivery of the Services. Policies include appropriate ramifications for non-compliance.

Risk Management

Cora takes a systematic approach to information security risk management not only to meet contractual and regulatory requirements, but also to satisfy the requirements of ISO, SOC 2, and Cyber Essentials. Our information security risk management methodology includes repeated risk assessments, allowing Cora Management to identify and prioritise the risks to be addressed. These assessments guide Cora’s risk mitigation strategies in response to new and evolving security threats.

Certifications

Cora maintains appropriate industry certifications and attestations. In addition, Cora requires IT vendors to have and maintain ISO27001 certifications. Cora contacts our vendor’s annually to ensure all certifications are up to date.

Audit

Customer audit rights with respect to the Services can be found in the Cora Data Protection Appendix.

Physical, Technical and Environmental Access Controls

Physical Access Measures

Cora limits physical access to its information systems and facilities to Cora IT Support personnel using physical controls. These shall include a combination of any of the following: CCTV systems, alarm systems, magna locks, pressure sensitive doors, access cards, biometric controls, on-site guards, intruder detection systems, sign in/out procedures, visitor escorting, log review processes.

In addition, Cora applies air temperature and humidity controls for its Communications room and protects against loss due to power failure.

Logical Access Controls

Cora uses logical access controls to restrict access to Cora IT infrastructure to authorized users. The guiding principle to these processes is that of strict need to know and least privilege.

Access to Cora SaaS software offerings is protected by authentication and authorisation mechanisms. SAML and Two factor authentication (email) are available. User authentication is required to gain access to all software offerings. Individuals are assigned a unique user account which is role based and requires login to the application. Access privileges are based on job requirements using the principle of least privilege access.

Cora employs monitoring and logging technology to help detect and prevent unauthorized access attempts to its networks and production systems.

Threat and Vulnerability Management

Cora utilises a number of network monitoring tools to ensure integrity and performance on our network. Monitoring software is installed on all Cora production environments. This allows Cora to monitor the entire IT infrastructure including our hosts, processes, and network for threats and vulnerabilities. It allows us to surface information such as total traffic of our network, Network availability, CPU usage of our hosts and response times of our processes. In this way, Cora maintains full visibility of host health, network performance, system performance and code issues in Cora PPM. Cora utilizes ‘Real User Monitoring’ functionality allowing Cora to gain full visibility into customer experiences across every digital transaction from frontend to backend.

Cora maintains anti-virus, end point security software to deliver centrally managed defences with integrated capabilities like endpoint detection and response and machine learning analysis. This protects Cora Microsoft OS and Mac systems with multiple, collaborative defences and automated responses. Additionally, Cora’s mobile device management software provides protection for Cora Mobile devices.

Malware Protection

Cora employs automated industry standard tools to continuously monitor workstations, servers, and mobile devices for active, up-to-date anti-malware protection with anti-virus, antispyware, personal firewalls, and host-based IPS functions. All equipment used by Cora is protected by a centrally managed endpoint security solution. This is used to scan all in-coming and out-going data for viruses, malware etc. Updated definition files are pushed out to all laptop/computers on a nightly basis.

External Devices

Cora operates a ban on external devices such as USB keys for the transfer of information.

Firewall

An industry standard firewall is installed and managed to protect Cora. Firewalls are set up to filter unauthorized inbound traffic from the Internet and are configured to deny inbound network connections that are not explicitly authorized by a rule.

Data Segregation

Cora maintains separate environments for production and non-production systems.

Each customer gets:

1) Dedicated infrastructure for that customer.

2) Dedicated and unique IP address and DNS entry.

3) IP Restrictions and whitelisting can be deployed.

These Data Segregation commitments do not apply to customers who are hosting the software on their own infrastructure.

Change Control

Cora change control policy ensures the effective management of change while reducing risk. Key components to the company's Change Management program include:

- Accurate Documentation
- Continuous Oversight
- Scope definition
- Formal, Defined Approval Process

Encryption

Cora utilises industry standard encryption to encrypt customer data at rest and customer data in transit. The customer gets end to end encryption of their data using secure a Https connection using TLS 1.2 cryptographic protocols and are encrypted using SSL certificate with RSA2048 (SHA256withRSA) bit encryption. All data at rest is encrypted using mainstream drive encryption which provides protection for Cora infrastructure as well as the data stored on it.

Penetration Testing

Cora initiates an annual penetration testing exercise to ensure the processes and procedures in place are robust in stopping attacks and responding quickly and effectively to scenarios. This annual penetration test is performed by a third party. The resulting Executive summary report is provided to customers upon request.

Cora customers may request to perform their own Penetration test on the Cora software offerings, at their own expense and only once per year. Facilitating customer requested Penetration tests may incur a fee.

Workstation security

Cora implements and maintains security mechanisms on employee laptops, including Firewalls, anti-virus, and full disk encryption using mainstream drive encryption. Cora operates a least privilege access policy.

Secure Code Review

Cora performs a combination of static and dynamic testing of code prior to the release of code to customers. Vulnerabilities are addressed in a timely manner. Software patches and new releases are regularly made available to customers to address known vulnerabilities and these are subject to quality review prior to release.

Illicit Code

Cora's subscription service offering shall not contain viruses, malware, worms, date bombs, time bombs, shut-down devices, that may result in, either: (a) any inoperability of Cora software offerings; or (b) any interruption, interference with the operation of the Cora software offerings. If Cora software offerings are found to contain any Illicit Code that adversely affects the performance of Cora software offerings or causes a material security risk to customer Data, Cora shall, as customer's exclusive remedy, use commercially reasonable efforts to remove the Illicit Code or to advise and assist customer to remove such Illicit Code. Cora is not responsible for Illicit Code introduced by customer, a third party, or sources other than Cora.

Company Security Measures

Asset Control

Cora records not only the type of software installed on each system, but also its version number and patch level. These details are tracked using an asset management tool. This tool allows Cora IT administrators to monitor all changes in software, hardware, licences and device allocation.

Wireless Network

Cora maintains an authorised configuration and security profile for each wireless device connected to the network. Devices without the profile shall not be allowed on the wireless internal network.

Email Management

Cora uses mainstream subscription services to manage our emails. Security and Compliance scans are employed for all emails that enter and exit a mailbox.

Personnel Security

Employees are subject to background checking, security screening, employment and education verification processes as part of the terms of their employment with Cora.

Security awareness and Data Protection Training

Security Awareness training and Data Protection Training is a requirement for all Cora employees at the time of hire and refresher training is carried out throughout their employment with Cora. These trainings include, among other things, phishing email awareness training, cyber security awareness training and invoice misdirection training.

Vendor risk management

Cora conduct vendor risk management assessments of its hosting and backup solutions providers annually. This is in addition to aforementioned vendor-related security commitments and risk mitigation strategies including confirmation of attestations, contractual assurances, and full infrastructure vulnerability analysis.

Business and Service Continuity

Backups

Data is automatically compressed, encrypted, and securely transmitted via the Internet to an offsite data centre. Data is also mirrored to a secondary data centre to provide a protective layer of redundancy. Our backup process, utilises 256-bit SSL encryption which safely secures data during transport over the Internet. Backups also have 256-bit AES encryption which safely secures data on the backup servers.

These Backup commitments do not apply to customers who are hosting the software on their own infrastructure.

Disaster recovery

Cora maintains a Disaster Recovery and Business Continuity Plan outlining Cora's response in the event of a disaster occurring at Cora offices or their environs. These are documented, approved, updated, and reviewed by management.

Service Continuity

Cora's Service Continuity Plan is engaged in the event of a disruption of service of our software offering to our customers.

Monitoring and Incident Management

Incident Management

Cora operates and maintains an Incident management policy. Cora will monitor, manage and respond to incidents in a timely manner, tracked via the Cora helpdesk and in line with current Service Levels.

Data breach

Cora operates a data breach process in line with the General Data Protection Regulation as described in the Cora Data Processing Appendix. Cora will contact the customer regarding any accidental, loss or destruction of, alteration, unauthorised disclosure or access to customer data in a timely manner, following determination by Cora that a data breach has occurred.

Cookies

Cora cookie policy is outlined in the below link

https://corasystems.com/cookie-preferences/

Limitations

Notwithstanding anything to the contrary in this Security Policy or other parts of the SSA, Cora obligations herein are only applicable to the Services as defined in the Subscription Service Agreement. This Security Policy does not apply to: (a) information shared with Cora that is not Customer Data; (b) data in customer's VPN or a third-party network; and (c) any data processed by customer or its users in violation of the Agreement or this Security Policy.