Cora Security Addendum

The Power of Perspective

Table of Contents

Information Security Addendum

This Information Security Addendum (ISA) sets forth the administrative, technical and physical safeguards Cora takes to protect confidential Information as part of its IT Security and Systems Management Policy. Cora may update this ISA from time to time to reflect changes in Cora ISP.

Cora Systems ("Cora") has adopted a security model in line with SOC 2 Type 2 international best practice standards. We exercise full control over all of our IT systems, being our infrastructure, networks, hardware, software which are used to manipulate process and store information. Cora also operates with a UK Cyber Essentials accreditation.

Cora IT framework which is used to manage and monitor the safety and security of our IT systems on a risk basis. We ensure uniform implementation of IT security controls throughout Cora, and appropriate oversight is given to meeting this aim. Cora contacts our vendor's annually to ensure all security Certifications are up to date.

Our security goals are:

- 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

Communicating these goals helps Cora reinforce the upkeep of our goals and policies throughout our organisation.

Application

Cora IT security policies apply to all employees (whether full or part time) in Cora and anyone working on a consultancy basis. Cora employees are subject to a security vetting process as per the Cora HR Background Checking policy. The Cora CST Team, 'Customer Success Team' are also BPSS 'Baseline Personnel Security Standard' cleared for enhanced security. We also use IT partners who we ensure have and maintain ISO27001 certification. We ensure their compliance with our requirements and with industry best practice.

Policies

Cora security policies are documented, reviewed and approved by management annually.

Risk Management

Cora has adopted a security model in line with SOC 2 Type 2. A systematic approach to information security risk management is necessary for Cora to identify the business needs to capture and manage information risk in order to meet contractual and regulatory requirements. In order to effectively manage information security risks, we have defined this methodology to reliably undertake repeated risk assessments, allowing Cora Management to identify and prioritise risks to be addressed.

Certifications

Cora security policies cover the management of security for both Cora internal operations and the services Cora provides to its customers, and apply to all Cora personnel, such as employees and contractors. These policies are aligned with SOC 2 Type 2 (or equivalent standards), and guide all areas of security within Cora. Cora also operates with a UK Cyber Essentials certification.

Physical, Technical and Environmental Access Controls

Cora utilises the security provisions of Microsoft Azure as its physical data centre operator to ensure industry standard best practises. Microsoft Data Centres hold both ISO 27001 and SOC2 controls.

Cora limits physical access to its own information systems and facilities using physical controls (e.g., coded badge access) that provide reasonable assurance that access to its Communications room is limited to Cora IT Support personnel. Cora employs CCTV systems at entry/exit points to its offices. Cora applies air temperature and humidity controls for its Communications room and protects against loss due to power failure. An Intruder alarm, magna locks, pressure sensitive doors are installed in Cora Offices. The Cora security team ensures their business partners, in the provision of Cora SaaS software solution also have adequate physical security infrastructure in place (e.g., access cards, biometric access controls, manned data centre security, intruder detection systems, sign in/out procedures, visitor escorting, CCTV, and log review processes in place)

Logical Access Controls

Protecting access to IT systems and applications is critical to maintain the integrity of Cora technology and data and prevent unauthorised access to such resources.

Access to Cora IT infrastructure is restricted to only authorized users or processes, based on the principle of strict need to know and least privilege.

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

All internal Cora systems require the use of MFA for staff to access.

Access to Cora SaaS software offerings, is protected by authentication and authorisation mechanisms. SAML and Two factor authentication. User authentication is required to gain access to all software offerings. Individuals are assigned a unique user account which is role based and requires a licence to login to the application. Individual user accounts shall not be shared. Access privileges are based on job requirements using the principle of least privilege access.

Threat and Vulnerability Management

We utilise several network monitoring tools to ensure integrity and performance on our network.

These include leading SIEM (Security Information and Event Monitoring), Endpoint Detection and Response, vulnerability scanning and misconfiguration detection providers.

Malware Protection

Cora uses Endpoint Detection and Response agents on all our assets. These agents are automatically updated multiple times per day to ensure that they are up to date with the latest threats, and have the latest methods of malware detection enabled.

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 (contract depending)
2) Dedicated and unique IP address and DNS entry
3) IP Restrictions and whitelisting can be deployed

Backups

Backups of customer data are carried out daily with a 1-month retention as standard. All backups have 256-bit AES encryption.

Change Control

Ensuring effective change management within the company's production IT environment is extremely important in ensuring quality delivery of IT services. 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, both on company servers and employee workstations is encrypted using mainstream drive encryption which provides protection for Cora infrastructure as well as the data stored on it.

Penetration Testing

Cora will initiate 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 can be provided to the customer 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, vulnerability management and full disk encryption using mainstream drive encryption. Cora operates a least privilege access policy.

GDPR ‘General Data Protection Regulation’

Cora is committed to the security of all data contained within its systems, including personal data and business data belonging to its customers. Cora is aware of its obligations and responsibilities in this area. Above all Cora prioritizes working with customers in relation to their security and specific data protection requirements.

Secure Code Review

Cora will perform a combination of static and dynamic testing of code prior to the release of code to customers. Vulnerabilities shall be addressed in a timely manner. Software patches and new releases are regularly made available to customers to address known vulnerabilities and go through a strict quality review prior to release.

Illicit Code

Cora’s software offerings 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.

Company Security Measures

Asset Control

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

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. We also employ an additional security provider on top of the default service settings to increase our protection.

Personnel Security

All 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 annually. Phishing email awareness training, cyber security awareness training and invoice misdirection training are all carried out.

Vendor risk management

Cora conduct vendor risk management assessments of its hosting and backup solutions providers annually.

Business and Service Continuity

Disaster recovery

Cora has both a Service continuity plan and a Disaster Recovery and Business Continuity Plan. The purpose of the Disaster Recovery Plan maintained by Cora is to outline Cora's' response in the event of a disaster occurring at Cora offices or their environments. These plans are reviewed annually.

Service Continuity

The service continuity plan is engaged in the event of a disruption of service of our software offering to our customers. The terms and conditions by our customers in relation to the use of our software offerings is set out in the customer contract and related documents.

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 agreed SLA's.

Data breach

Cora operates a data breach process in line with GDPR 'General Data Protection Regulation'. 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 Cora ISA or other parts of the Agreement, Cora obligations herein are only applicable to the Cora software offerings. This ISA 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 ISA.