CarbonCloud

Security Overview

Code:	ISMS-0020
Version:	2.3
Date of version:	2025-02-13
Created by:	Annika Gunnarsson
Approved by:	David Bryngelsson
Confidentiality level:	Public use

Introduction

At CarbonCloud, we understand that the security and privacy of your data is of paramount importance. As a trusted SaaS provider, we have implemented comprehensive security measures across our organization, infrastructure, and application to protect your information. This document outlines our security practices and controls.

Organizational Security

Security Team

Our dedicated security team is led by the Head of Engineering who oversees all security initiatives and ensures compliance with industry standards and regulations.

Employee Security

- **Security Training**: Employees receive comprehensive security awareness training upon hiring and regular ongoing training.
- **Access Controls**: We implement the principle of least privilege, ensuring employees only have access to the resources necessary for their job functions.

Infrastructure Security

Data Centers

- Our application is hosted in AWS data centers, which maintain ISO 27001, and other relevant certifications.
- Physical access to data centers is strictly controlled with multi-factor authentication, 24/7 surveillance, and security personnel.

Network Security

- **Firewalls**: Enterprise-grade firewalls protect our network perimeter.
- **Intrusion Detection/Prevention**: Real-time monitoring systems detect and block suspicious activities.
- **Network Segmentation**: Our network is segmented to limit lateral movement in case of a breach.
- **DDoS Protection**: We employ advanced DDoS mitigation techniques to ensure service availability.

System Security

- **Patch Management**: All systems are regularly updated with the latest security patches.
- **Vulnerability Management**: We conduct regular vulnerability scans and remediate findings based on risk.

- **Endpoint Protection**: All endpoints are protected with advanced anti-malware solutions.
- **Hardened Configurations**: Systems are deployed with hardened configurations based on industry best practices.

Application Security

Secure Development

- **Secure SDLC**: Our development follows a secure software development lifecycle.
- **Code Reviews**: All code changes undergo peer review before deployment.
- **Static and Dynamic Analysis**: Automated tools scan code for security vulnerabilities.
- **Penetration Testing**: Regular penetration tests are conducted by independent third parties.

Data Protection

- **Encryption in Transit**: All data transmitted to and from our application is encrypted using TLS 1.2 or higher.
- **Encryption at Rest**: Customer data is encrypted at rest using AES-256 encryption.
- **Data Segregation**: Customer data is logically segregated to prevent unauthorized access.

Authentication and Access

Customer Application Access

- **Single Sign-On**: Support for enterprise SSO solutions (SAML, OIDC) for customer organizations.
- **Password Policies**: Enforcement of strong password requirements for all customer accounts.
- **Session Management**: Automatic session timeouts and secure session handling for customer sessions.

Internal Access Controls

- **Privileged Access Management**: Strict controls on administrative and system access.
- **Multi-Factor Authentication**: Mandatory MFA for all employee accounts and internal systems.
- **Role-Based Access Control**: Granular permissions based on job responsibilities.
- **Just-in-Time Access**: Temporary elevated privileges with approval workflows for sensitive operations.
- **Access Reviews**: Regular reviews of access rights and prompt removal upon role changes or departures.

Operational Security

Monitoring and Logging

- **24/7 Monitoring**: Continuous monitoring of systems, networks, and applications.
- **Centralized Logging**: All logs are collected and analyzed in a centralized SIEM solution.
- **Alerting**: Automated alerts for suspicious activities or potential security incidents and application health.

Incident Response

- **Incident Response Plan**: Documented and regularly tested incident response procedures.
- **Response Team**: Dedicated team ready to respond to security incidents.
- **Communication Protocol**: Clear protocol for notifying affected customers in case of incidents.

Disaster Recovery & Business Continuity

- **Backup Strategy**: Regular backups with secure off-site storage, infrastructure in version controlled IaC.
- **Disaster Recovery**: Comprehensive DR plan with regular testing.
- **Redundancy**: Systems designed with redundancy to eliminate single points of failure.

Third-Party Risk Management

- **Vendor Assessment**: Rigorous security assessment of all third-party vendors.
- **Contractual Requirements**: Security and privacy requirements included in all vendor contracts.
- **Ongoing Monitoring**: Regular review of vendor security posture.

Contact Information

For more information about our security program or to report security concerns, please contact:

- **Security Team**: security@carboncloud.com

This document is provided for informational purposes to current and prospective customers. While the information can be shared within your organization, please contact CarbonCloud for the most current version of this document when needed.