Credly

Data Security Brief

Last Updated August 2020

Overview

Introduction

Credly was founded to help people get recognition for their skills, to connect their verified abilities to opportunities, and to bring happiness, equity, and access to every member of the current and future workforce. That mission aligns with a larger global trend of empowering individuals with control over their own data. Our policies and processes operationalize that commitment to ensuring the security and privacy of our customers and their employees, members, learners, and users. We invest in best practices and compliance with industry standards. All Credly employees are trained in data security and privacy principles.

Protecting customers and their users is our top priority and we emphasize data security in everything that we do. Our approach has enabled Credly to serve many of the world's most trusted and recognizable brands as the industry standard provider of digital credential services and home to the largest network of verified credentials in the world.

This document explains how Credly safeguards the data provided to Credly by its customers about their employees, users, members, students, and certification earners (what we call "Issuer Data"). We are proud to offer the industry-standard solution for digital credentials and we hope this document inspires your confidence.

Credly Information Security Standards

Credly employs appropriate technical and organizational measures to protect customer data ("**Issuer Data**") from unauthorized or unlawful processing, loss, destruction or damage. Credly's Information Security Program includes specific security requirements for all personnel and subcontractors who have access to Issuer Data. You can view the Credly Information Security Standards via the Credly Data Processing Addendum (see Annex 1).

Information Security Policies and Standards.

Credly maintains a variety of information security policies, standards, and procedures. These policies, standards, and procedures are kept up to date and revised whenever relevant changes are made to the information systems that use or store Issuer Data. All policies and procedures are reviewed and updated at least annually. These policies, standards, and procedures shall be designed and implemented to:

- Prevent unauthorized persons from gaining physical access to Issuer Data (e.g. physical access controls)
- Prevent Issuer Data from being used without authorization (e.g. logical access control)
- Ensure that personnel with access to personally identifiable information (**"Personal Data"**) gain access only to such Personal Data as they are entitled to access (e.g. in accordance with their access rights) and that, in the course of processing or use and after storage, Issuer Data cannot be read, copied, modified, or deleted without authorization (e.g. data access controls)
- Ensure that Personal Data cannot be read, copied, modified, or deleted without authorization during electronic transmission, transport or storage, and that the recipients of any transfer of Issuer Data by means of data transmission facilities can be established and verified (e.g. data transfer controls)
- Ensure the establishment of an audit trail to document whether and by whom Personal Data has been entered into, modified in, or removed from Personal Data processing (e.g. entry controls)
- Ensure that Personal Data is processed solely in accordance with Issuer's instructions (e.g. control of instructions)
- Ensure that Issuer Data is protected against accidental destruction or loss (e.g. availability controls)
- Ensure that Personal Data collected for different purposes can be Processed separately (e.g. separation controls)
- Ensure that Personal Data maintained or processed for different customers is Processed in logically separate locations (e.g. data segregation)
- Ensure that all systems that Process Issuer Data are subject to a secure software development lifecycle
- Ensure that all systems that Process Issuer Data are the subject of a vulnerability management program that includes without limitation internal and external vulnerability scanning with risk rating findings and formal remediation plans to address any identified vulnerabilities.

Physical Security

- **Physical Access Controls.** The Credly System is hosted in a datacenter located at nondescript facilities owned and operated by a third-party hosting provider (the **"Facilities"**). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.
- **Limited Employee and Contractor Access.** Credly's hosting provider provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges.

When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of Credly's hosting provider or its Affiliates.

- **Physical Security Protections.** All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. Credly's hosting provider also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

Organizational Security

Credly maintains information security policies and procedures addressing the below indicated areas. Applicable policies are available for review online.

- **Data Disposal.** Procedures for when media are to be disposed or reused have been implemented to prevent any subsequent retrieval of any Issuer Data stored on media before they are withdrawn from the Credly's inventory or control.
- **Data Minimization.** Procedures for when media are to leave the premises at which the files are located as a result of maintenance operations have been implemented to prevent undue retrieval of Personal Data stored on media.
- **Data Classification.** Policies and procedures to classify sensitive information assets, clarify security responsibilities, and promote awareness for all employees have been implemented and are maintained.
- Incident Response. All Issuer Data security incidents are managed in accordance with appropriate incident response procedures.
- **Encryption.** All Issuer Data is stored and transmitted using industry standard encryption mechanisms and strong cipher suites, such as AES-256.

Network Security

Credly System is hosted in a datacenter located at nondescript facilities owned and operated by a third-party hosting provider. Credly does not maintain an internal network. The Credly engineering team makes use of industry standard virtual private networks (**"VPN"**) to manage infrastructure resources and access the Credly System.

Access Control (Governance)

- Credly governs access to information systems that process Issuer Data.
- Only authorized Credly staff can grant, modify, or revoke access to an information system that processes Issuer Data.

- User administration procedures are used by Credly to: (i) define user roles and their privileges; (ii) govern how access is granted, changed, and terminated; (iii) address appropriate segregation of duties; and (iv) define the requirements and mechanisms for logging/monitoring.
- All Data Personnel are assigned unique User IDs.
- Access rights are implemented adhering to the “least privilege” approach.
- Credly implements commercially reasonable physical and technical safeguards to create and protect passwords.

Virus and Malware Controls

Credly protects Issuer Data from malicious code and will install and maintain anti-virus and malware protection software on any system that handles Issuer Data.

Personnel

- Credly has implemented and maintains a security awareness program to train all employees about their security obligations. This program includes training about data classification obligations, physical security controls, security practices, and security incident reporting.
- Credly has clearly defined roles and responsibilities for employees.
- Prospective employees are screened, including background checks for Data Personnel or individuals supporting Issuer’s technical environment or infrastructure, before employment and the terms and conditions of employment are applied appropriately.
- Personnel with access to Personal Data strictly follow established security policies and procedures. Disciplinary process up to and including termination is applied if such personnel fail to adhere to relevant policies and procedures.
- Credly takes reasonable steps to ensure the reliability of any employee, agent or contractor who may process Personal Data.

Business Continuity

Credly implements disaster recovery and business resumption plans. Business continuity plans are tested and updated regularly to ensure that they are up to date and effective.

Additional resources

Publicly Available

- Data Privacy & Security Credentials
- Privacy Overview
- GDPR FAQ
- Credly Data Protection Addendum (DPA)
- Credly Information Security Standards (see Annex 1)
- Privacy Policy

- Uptime Reporting

Videos & Podcasts

- Video: What Happens to Your Data When You Issue Digital Credentials
- Podcast: What Does it Take to have Enterprise Level Security

Available under Non-Disclosure Agreement

- Penetration Testing Results
- Data Security Policies & Procedures
- Business Continuity and Disaster Recovery Plans and Test Results
- Completed Higher Education Community Vendor Assessment Toolkit (HECVAT)
- Completed Vendor Security Alliance (VSA) Questionnaire