blacklinesafety

Data Security and Privacy Policy

Approved November 30, 2018 and amended on March 23, 2021

Background

Blackline Safety Corp. and its subsidiaries (collectively, "Blackline" or the "Company") is committed to ensuring that the information entrusted to us by our customers and staff is handled in such a way that it is secure, and privacy is maintained. Customer and staff identifiable information will only be used for legitimate business purposes and may be shared with our data partners.

We will ensure that both customers and staff have a method of contacting the Blackline Safety Privacy Officer and staff tasked with maintaining adequate security for their information.

The following email address has been set up for contacting Blackline Safety with any privacy, security or requests for access, modification or deletion of personal information held by Blackline Safety privacy@blacklinesafety.com

Data security and privacy is the responsibility of all Blackline staff with access to data bases containing identifiable information. As such all Blackline staff will undergo training on privacy and data security. All staff will sign the Blackline Confidentiality, Intellectual Property and Conflict of Interest Agreement which prohibits communication of identifiable information other than for legitimate business interests.

Verification of Identity

All staff will adhere to the Identity verification and information release procedure when dealing with requests for information, change requests or right to be forgotten requests, originating outside of Blackline. All requests will be logged on tickets generated by Customer Support or internal emails generated by SOC outside of normal office hours.

Data Incidents

Any actual, suspected or potential compromise of data or customer concern regarding their data held by Blackline Safety will be dealt with according to the Data Incident Report work instructions.

Qualification of Staff

Blackline will ensure that all staff are suitably qualified and trustworthy to handle identifiable information. Staff who are not members of professional bodies will have a police background check completed prior to being given access to identifiable information. Qualifications and information access levels will be documented on the Interview record form. Employees working with Blackline Safety prior

to October 2018 will be classed as acceptable based on their performance and integrity displayed while working with the company.

Data Access Levels

Initial data access levels will be documented on the Interview record form, this form will be used by IT to grant the required access and returned to People Services when completed.

d) Where there is a requirement to grant additional access to a current employee the request is to be submitted to IT using the Data Access Level form. The form must be authorized by the Senior Department Manager, Privacy Officer or Risk and Compliance Officer. IT will return the form to People Services once the access has been granted.
e) When access is no longer required, or the employment contract is terminated access privileges to the system are to be removed immediately; ensuring that there is no opportunity for unauthorized access. The date and time of removal is to be noted in the employee file.

Data Security

The primary means of intrusion / un-authorized access detection are Acunetix and Threat Stack. The primary point of contact for alerts is the Software Security Architect designate. The Software Security Architect or designate logs into Acunetix and Threat Stack periodically and reviews /acknowledges the event logs.

System Audit

The Risk and Compliance Officer will conduct an audit of all processes and procedures used to ensure data security and privacy. The audit may be done as a system audit or an audit of individual procedures used. As a minimum every process will be audited annually.

System Review

Periodic compliance meetings are targeted to be held weekly and are chaired by the Software Security Architect. This meeting is attended by the RCO, Project Manager and the Software Manager and reviews the progress towards any information security related topics. Minutes for this meeting are maintained by the Software Security Architect. The implementation and performance of the Information security processes and procedures is included in the twice-yearly management review meetings. Details of discussions are contained in the minutes for each meeting.