blacklinesafety

TRUST PACKAGE 2024

PRIVACY, SECURITY AND COMPLIANCE

blacklinesafety.com

TABLE OF CONTENTS

INTRODUCTION

Blackline Safety (Blackline) is committed to upholding the highest standards of worker privacy and data security. We meticulously adhere to industry best practices to safeguard both worker and customer data, ensuring its utmost protection. In our continuous efforts to establish trust, we offer customers a comprehensive security documentation package that thoroughly addresses frequently asked questions and concerns related to security. For any additional inquiries or information, please do not hesitate to reach out to us via phone or email. Your trust and data security are our top priorities.

ABOUT BLACKLINE SAFETY

Blackline is a technology leader driving innovation in the industrial workforce through IoT (Internet of Things). With connected safety devices and predictive analytics, Blackline enables companies to drive towards zero safety incidents and improved operational performance. Blackline provides wearable devices, personal and area gas monitoring, cloud-connected software and data analytics to meet demanding safety challenges and enhance overall productivity for organizations with coverage in more than 100 countries. Armed with cellular and satellite connectivity, Blackline provides a lifeline to tens of thousands of people, having reported over 250 billion data-points and initiated over eight million emergency alerts. Blackline offers an optional 24/7 live monitoring Safety Operations Center (SOC) to provide organizations with real-time coverage and peace of mind to keep workers safe around the clock. Our in-house SOC and global monitoring partners ensure professional and reliable safety monitoring and emergency response management.

BACKGROUND

This trust document explains Blackline's commitment to security, privacy and compliance. It covers the purpose of Blackline's products and services, the information we process or store for you, and the importance of our service availability to your business. Additionally, we consider the legal, regulatory, and contractual requirements for the information you share with Blackline.

BLACKLINE SAFETY CLOUD

Blackline develops IoT cloud software (Blackline Cloud) and services that monitor employee safety across various locations. The Blackline Cloud includes:

- Software
- Networking
- Provisioning
- Data storage
- Customer accounts with access controls
- Blackline Live user portal
- Device service subscription management
- Reporting

We use modern cloud-based infrastructure technologies to build, maintain and innovate new software features for our connected safety devices. The Blackline Cloud is a fully independent software platform that does not require data access to any external client data sources or services.

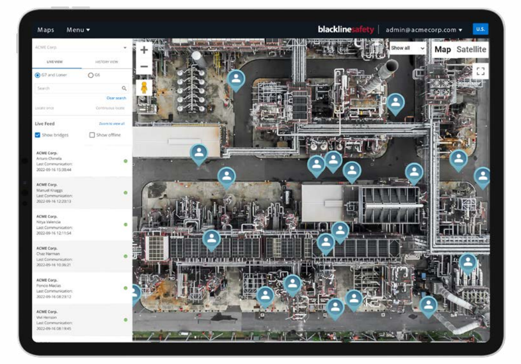
The Blackline Cloud is hosted by Amazon Web Services (AWS), a leading cloud hosting service provider. Global brands like 3M, BP, Adobe, Canon, GE, Alcatel Lucent, BMW, Hitachi, NASA and many others trust and rely on AWS for hosting, virtualization, data backup and other online services.

BLACKLINE LIVE

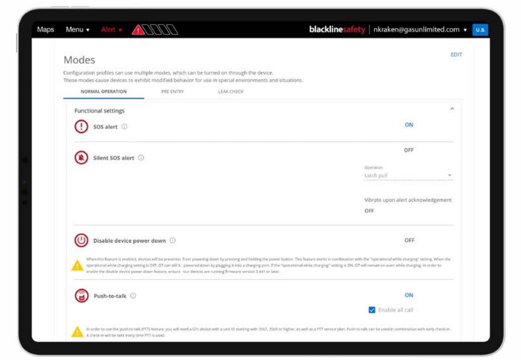
As part of the Blackline Cloud, Blackline Live is our web-based user portal that supports:

- IoT safety device assignment
- Device configuration management
- Alert configuration
- Alert lifecycle management
- Data analytics

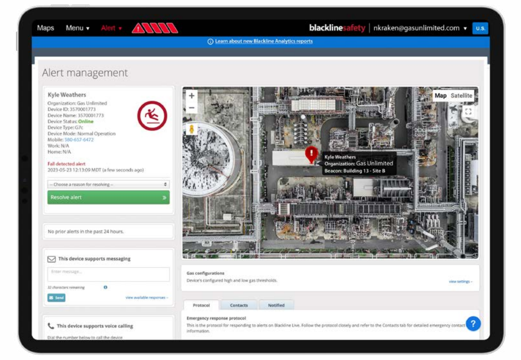
The portal also supports role-based access controls to ensure personnel only have access to approved information and device grouping capability with corresponding access controls, plus the ability to link multiple Blackline Live organization-level accounts together.



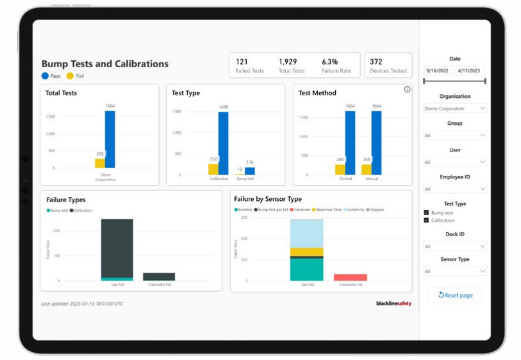
Blackline Live Map



Blackline Live Configurations



Blackline Live Alert Management



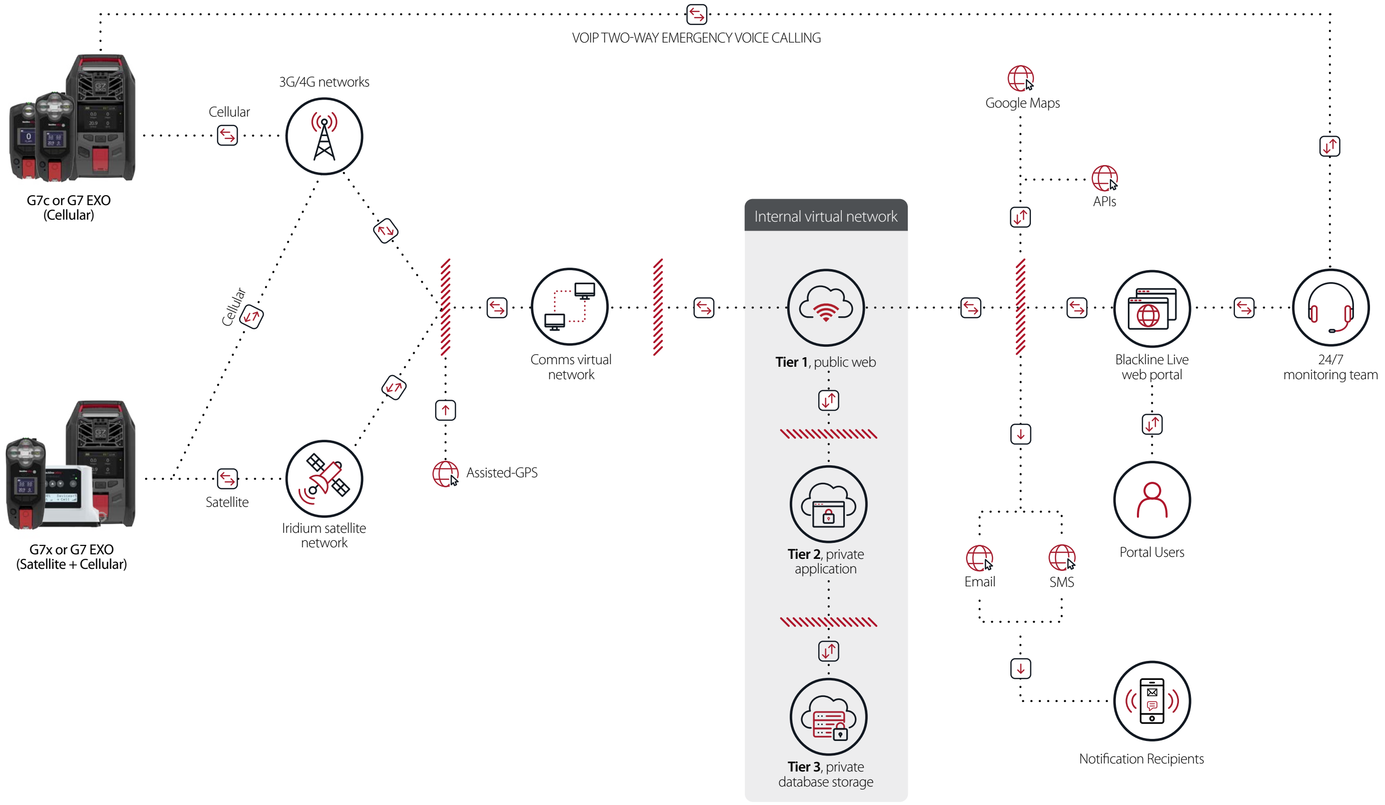
Blackline Analytics - Bump Tests and Calibration

BLACKLINE CLOUD ARCHITECTURE

Blackline's safety IoT devices communicate directly with the Blackline Cloud using cellular (2G, 3G, 4G, NB-IoT, and LTE-M) and optional satellite connectivity. Our IoT devices do not require connection into traditional customer IT networks, such as Wi-Fi. Cellular services are offered in most countries and territories globally, while satellite communications are limited to North America, some Central and South American countries, Australia, New Zealand and South Africa.

Our Blackline Live user portal is the primary interface for safety IoT device configuration, alert setup, emergency response management and reporting. We also provide software APIs for real-time alert delivery and IoT safety device information retrieval.

The Blackline ecosystem comprises connected safety devices, communications networks, cloud-hosted infrastructure, user interfaces and live monitoring personnel. Within the Blackline Cloud, we have established separate virtual networks for device traffic, communications networking, internal network, core application and data storage. These layers are each firewalled from one another to ensure control throughout the complete architecture.



LEGEND | FIREWALLS: ▨ | WEB SERVICES: 🌐 | DATA FLOW: · · ⇆ · · · |

BUSINESS-CRITICAL SERVICE AVAILABILITY

Each customer must assess the criticality of Blackline's services to its business. As a safety monitoring system, Blackline recommends a comprehensive internal review and assessment of the system, including how to manage continuity of safety monitoring in the event that our cloud services are temporarily unavailable. A client's operations, legal, and compliance teams are likely the best resources equipped to support this assessment. A copy of our Service Level Agreement (SLA) is available upon request.

PERSONAL INFORMATION

Blackline safeguards client data with comprehensive policies and procedures designed to protect this information. Please refer to our Privacy Policy for more details.

Our services include access to our Blackline Live user portal, wireless connectivity, cloud-based data storage, Blackline Analytics reporting, email/text notifications, and options like alert management, two-way emergency voice calling, push-to-talk and software APIs. Some services require password-protected Blackline Live user account access.

Under our services, we may collect, store and process confidential information, including employee personal identifiable information (PII). For PII, clients operate as data controllers while Blackline acts as the processor. Overall customer information, including PII, may include:

- Organization name and address
- Employee names, roles, employee IDs, phone numbers, locations, addresses, and emails (PII)
- Employee personal contacts with names, phone numbers and relationship types (PII)
- Documented emergency response protocols
- Location Beacon names, locations and addresses
- Site and/or floor plan layers
- Assignment of devices to employee contact cards stored within the address book (PII)
- Alert profiles that define alert logic based upon device settings, plus notification subscribers from the employee address book (PII)
- Alert management history with employee name, timestamps, locations, notations (PII)
- Emergency voice calls recorded through Blackline's Twilio service vendor (PII)
- Safety Operations Center recorded voice calls from our global contact center partner and stored in Azure (PII)
- Two-way messages between device users and the monitoring team (PII)

To provide customers with information and services, Blackline may use this information to:

- Establish a contract with our customers, including verification of employee identities as required to process payments, provide implementation services and support users.
- Monitor the use of our websites and online services, helping us check, improve and protect our products, content, services and websites.
- Respond to any comments or complaints we may receive from our customers about our website, products, or services.
- Provide our customers with information about new products, product and service updates, newsletters, informative emails, and research on future product ideas or improvements, as well as to personalize our communication to our customers.
- Invite our customers to take part in market research or surveys.

Customer information collected through the Blackline Live websites will be anonymized following termination of a client's services, and aggregated to allow us to improve our services. Information collected through our marketing website, www.blacklinesafety.com, is collected and managed according to our Privacy Policy. All confidential information and PII provided by our clients is never shared with third parties beyond sub-contracted vendors that assist in delivering our products and services to clients.

LEGAL, REGULATORY, AND CONTRACTUAL REQUIREMENTS

Determining the legal, regulatory, or contractual constraints for your PII and other information processed by the Blackline Cloud is your responsibility in collaboration with your, legal and compliance teams. Most customers consider this data confidential. If you have users located in the European Economic Area (EEA), General Data Protection Regulation (GDPR) privacy requirements may apply to PII shared with Blackline.

Storing or processing any sensitive personal information beyond basic employee details (e.g., names, phone numbers, email addresses, physical addresses, geographic locations, and environmental status) is not recommended on our platform. This includes personal health information (PHI) and payment information like credit card numbers. Consequently, Blackline does not support HIPAA or PCI-DSS compliance.

OVERVIEW

Securing trust with our customers is supported by four pillars: information security, compliance, privacy, and reliability.

1. Information security

INFORMATION SECURITY MANAGEMENT

Blackline has developed an Information Security Management System (ISMS) and Information Security Policy (ISP) to ensure a comprehensive and organized approach to information security. The ISMS framework includes controls aligned with the Trust Services Principles and Criteria for Security and Availability, essential for maintaining Blackline's Service Organization Controls (SOC 2) Type 2 audit report.

CORPORATE AND OPERATIONAL SECURITY

Production infrastructure access: Access to the production infrastructure requires authentication through a cryptographic authentication key over a secure encrypted protocol (SSH). It also mandates the authentication requests originate from a known set of IP addresses, and all user accounts require a unique identifier.

Production application access: Only authorized Blackline employees have application-level access to perform tasks like support, migration, and professional services. Access is provided through internal controls and processes.

Access reviews: In addition to automated controls, periodic access reviews are conducted on in-scope systems to limit administrative access to production systems based on approved roles and responsibilities.

Training and awareness: All Blackline employees receive security and privacy awareness training during onboarding, as well as ongoing refreshers. Training covers topics including information security, phishing awareness and prevention, password policy, security incident management, office physical security, confidentiality requirements and data privacy.

Corrective and preventive action: Blackline takes action to control and correct nonconformities or suspected control breakdowns through root cause investigations, implementing preventative measures and assigning the necessary resources within the timelines as required.

Change management procedures: To comply with SOC 2 requirements, Blackline has established formal change management processes to control the design, development, testing, and implementation of fixes and improvements to the Blackline Cloud and Blackline Live portal. These processes mitigate the risk of unauthorized changes to production systems and address the production infrastructure and software development lifecycle. They include change requests, approvals, and standard change implementation procedures for commonly applied changes.

Blackline Safety employees: Employees must sign an acknowledgment form confirming access to and review of the Employee Handbook, along with their understanding of the responsibility to comply with its security policies. Additionally, employees are required to sign a confidentiality and non-disclosure agreement (NDA) that prohibits the disclosure of proprietary or confidential information, including customer information, to unauthorized parties. Background checks, including criminal, education, and references are conducted as part of the hiring process.

PRODUCT SECURITY

Infrastructure: The Blackline Cloud is hosted and managed on Amazon Web Services (AWS) across multiple availability zones to support fault tolerance, high availability, and disaster recovery. Rackspace is used as a secondary hosting provider to store encrypted backups, thus mitigating the risk of a single infrastructure provider failure that could result in customer data loss. Blackline Vision, our data analytics team, also use Microsoft Azure and Power BI for reporting and data visualization.

Software development lifecycle: Before implementing changes in the production environment, Blackline software developers perform source code reviews along with security, functional, and performance testing for major application changes. Development and testing activities are conducted in separate test environments to eliminate the risk of production impact.

Encryption: To protect customers' confidential data, Blackline encrypts data in the Blackline Cloud and Blackline Live portal. Customer data is securely transferred to the Blackline Live portal using Transport Layer Security (TLS v1.2) and is encrypted at rest using AES256 encryption.

Key management: Blackline uses AWS Key Management Service (KMS) for encrypting our customer data. KMS is designed to prevent unauthorized access to master keys, ensuring the security of data stored within Blackline Cloud. Regular audits by third party assessors certify AWS KMS practices align with industry-best cryptographic standards.

Multi-tenancy: Blackline's platform is designed for multiple customers, providing consistent access and standardized processes. Logistical separation of customer data is achieved through a Role Based Access Control (RBAC) system. Access to data is restricted based on customer identifiers, and each record in the Blackline Cloud includes a unique customer identifier. User sessions are linked to customer identifiers, ensuring customer-specific data retrieval.

Admin-enabled access controls : The Blackline Cloud features a robust grouping structure in its permissions system. Customers can efficiently manage content access for specific users through Blackline Live groups. These groups function as containers, allowing customers to create a device grouping structure that aligns with their organization or site-based structure. Leveraging the RBAC system, customers have precise control over user access to designated groups, ensuring a tailored and secure content management experience.

Authentication: Blackline supports single sign-on (SSO) via SAML 2.0 compliant Identity Providers (IdPs). As long as an IdP uses SAML, Blackline can integrate with it. Additionally, multi-factor authentication (MFA) for Blackline Live is available through SSO when connected to a supported IdP. Blackline also supports form-based authentication.

Product security testing: For internal testing, Blackline performs Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) to detect security vulnerabilities, including all vulnerabilities outlined in the OWASP top-10. Additionally, specialized external third-party service firms are contracted for annual penetration tests to detect malicious code and other vulnerabilities. Results are reviewed by engineering and security staff who develop remediation plans for identified vulnerabilities.

2. Privacy

POLICY

Blackline maintains and publishes its Privacy Policy online at www.blacklinesafety.com, informing clients about its privacy practices that support customer objectives. Any changes to Blackline's privacy practices, including changes in the use of PII, are included in the policy to align with client privacy objectives.

CONSENT, COLLECTION AND PROCESSING

Blackline communicates the choices available to clients regarding the collection, use, retention, disclosure, and disposal of their personal information. We obtain explicit consent from clients for these activities, ensuring alignment with their privacy objectives and using the information only for its intended purpose. Blackline collects PII in accordance with its Privacy Policy, obtaining explicit consent prior to collection to meet privacy objectives. Blackline obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.

The use of personal information is limited to the purposes specified in the privacy objectives.

DATA RETENTION

Blackline retains data for three years after the lapse of contract unless shorter retention times are requested by the customer. The Blackline Live portal has 125 days of data available to the customer, and data older than 125 days is accessed via Blackline Analytics.

The current retention policy starts after a customer ends their services contract with Blackline. Three years after services termination, Blackline reserves the right to delete customer data.

System-wide encrypted backups are maintained for a revolving 30-day period in compliance with GDPR, with a maximum retention of 60 days before deletion.

USA AND EUROPE DATA RESIDENCY

Blackline offers two data residency options: USA and Europe, with separate live domains. This ensures that European customers' GDPR-regulated PII is stored within the European Blackline Cloud but also fully processed in Europe to meet their GDPR requirements.

Organizations with GDPR requirements are automatically set up in our European Blackline Cloud services. Blackline works with our customers' organizations to ensure that all data resides in the appropriate region for their organization, including companies that operate both inside and outside of Europe.

BACKUPS

Described earlier, Blackline uses Rackspace as a secondary hosting provider to store encrypted backups, mitigating the risk of a single infrastructure provider failure that could result in customer data loss. Customers can request a backup and export of their data within an encrypted file by contacting Blackline's Customer Care team at support@blacklinesafety.com.

THIRD-PARTY VENDOR DATA ACCESS

Blackline only discloses client PII to contracted third-party vendors for the purpose of delivering services to our customers. This includes the sending of SMS and email notifications and alerts that may include employee names, phone numbers, physical addresses and email addresses, geographic locations and environmental data. This also includes the hosting of the Blackline Cloud and associated information, including PII in AWS and Azure.

UNAUTHORIZED PRIVACY DISCLOSURES

Blackline creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the client's objectives related to privacy.

3. Compliance

Blackline's hosting providers, AWS and Microsoft Azure, undergo annual audits against widely recognized standards and frameworks such as SOC 1, SOC 2, and ISO 27001.

While many software-as-a-service (SaaS) companies solely rely on their hosting providers' security and compliance certifications, Blackline views information security as a shared responsibility. We hold ourselves to the highest industry standard for security assurance and undergo an annual SOC 2 Type 2 audit. This provides customers with an independent third-party assurance that our security controls are designed and operating effectively.

GDPR

To assist our European customers in achieving their GDPR compliance goals, Blackline established a dedicated European Blackline Cloud and Blackline Live portal. Customers with European operations can have their data processed and stored within EU borders in accordance with GDPR guidelines. Our European Blackline Cloud services and dedicated Blackline Live portal securely store all European customer transactional data, long-term data and PII entirely within European borders.

4. Reliability

Blackline is committed to providing high quality, reliable service, having designed the Blackline Cloud to leverage multiple datacenters and high availability.

MULTIPLE DATA CENTERS

Blackline's North American infrastructure is hosted and managed on AWS across multiple availability zones and regions for certain functions. This structure supports fault tolerance, high availability, and disaster recovery. Our primary site is in northern Virginia, USA, with a secondary site in Oregon, USA.

BUSINESS CONTINUITY AND DISASTER RECOVERY

Blackline has Business Continuity and Disaster Recovery plans to meet business and availability requirements. Blackline's Service Level Agreement (SLA) includes our availability commitments, maintenance policy, and technical support response times, including hours of coverage, and escalation. A copy of our SLA is available upon request.

H1 - HEADER -28

H2 - HEADER - 18

H3 - Header - 14

H4 - Header - 12

H5 - Headler -10

H6 - Header -8

Body Copy - Body copy

Call outs - Legal copy, diagram call-outs - Myriad Pro | Light | Size 6 | Lead 6 | Tracking +20 |
Fine print - Legal copy, diagram call-outs - Myriad Pro | Light | Size 6 | Lead 6 | Tracking +20 |

H3 - Headline with paragrah rule

Body Copy - Body copy character style - Myriad Pro | Light | Size 12 | Lead 14 | Tracking -20 |

Hyperlink

- Bulleting

1. Bulleting