Securing Information with Trust, Transparency, and Resilience

Information Security Summary

KLDiscovery's Vice President and Chief Information Security Officer operates with the full support and unqualified mandate of our CEO and Board of Directors to ensure that information security remains a top priority across the organization.

Culture

Security is embedded in every part of KLDiscovery's operations and culture. Our world-class Information Security team is supported by security champions embedded across departments, spanning software development, dynamic code analysis, and facility security. From day one, employees are trained to prioritize security, ensuring vigilance is built into every action we take.

> "Security leadership demands more than vigilance—it requires anticipating what comes next. At KLDiscovery, we architect our security programs with forward-looking strategies, rigorous operational discipline, and an unwavering drive to strengthen resilience at every level."

JASON DAVISON

Vice President and Chief Information Security Officer, KLDiscovery

Organization

KLDiscovery Information Security and Technology is structured around five critical pillars:

1. Security Architecture

KLDiscovery adheres to a defense-in-depth strategy where preventative, detective, and reactive controls are deployed to monitor and protect our system environments. Our security control framework is based on the NIST Cybersecurity Framework and is regularly assessed for maturity and updated as needed. In addition to NIST, we align with industry best practices, including those from OWASP, the Cloud Security Alliance, and the Software Assurance Maturity Model (SAMM).

2. Security Operations and Tools

KLDiscovery's security operations apparatus is focused on the effectiveness and completeness of our deployed security tools within a defense-in-depth strategy, alongside the active tracking and mitigation of vulnerabilities across the enterprise. We maintain a broad range of security controls and technologies designed to deliver resilient protection at every layer of our technology stack. Our foundation includes Intel Security and Cisco platforms, supplemented by best-of-breed technologies such as Palo Alto Networks and Carbon Black/Bit9 to guard against common and emerging threats. KLDiscovery's security capabilities include:

- Firewalls and intrusion prevention systems at all perimeter points, DMZs, VPNs, and internet egress gateways
- Two-factor authentication enforced for external VPN and corporate webmail access
- Dedicated anti-virus (AV) and intrusion prevention systems (IPS) protecting inbound email, with continuous metric tracking to drive improvement
- Endpoint protection featuring real-time malware signature updates, anomaly detection, and Indicators of Compromise (IOC) monitoring
- Proxy servers controlling end-user internet access, governed by an enforced Acceptable Use Policy

- Annual third-party penetration testing to validate system security posture
- Enterprise-wide Security Information and Event Monitoring (SIEM) system aggregating security events and logs for real-time incident response
- Weekly internal and external vulnerability scans with risk assessments and documented resolution tracking
- A 24/7 Security Operations Center (SOC) providing real-time health, performance, and anomaly monitoring
- Robust escalation and incident management procedures supported by on-call resources across all critical technology domains
- Active monitoring of all systems tied to authentication, including account creation, group membership access, and network device access
- Centralized platform management for prioritization and action on security alerts and logs

3. Incident Response

Our Incident Response team actively monitors for anomalous behaviors and potential threats across our systems. We operate under a defined Incident Command Structure (ICS) and leverage the VERIS framework for incident reporting, ensuring every event is captured, investigated, and addressed with precision.

4. Threat Intelligence

KLDiscovery's threat intelligence program continuously monitors public and private sources to stay ahead of emerging risks. This intelligence feeds directly into our operational defenses, helping us anticipate threats before they materialize.

5. Security Governance and Compliance

KLDiscovery established and maintains a Security Governance Program designed to meet best-in-class security practices, including education initiatives and strengthened security awareness across the enterprise. Our approach spans Governance, Policy, Controls, and Assurance, grounded in a Plan-Do-Check-Act (PDCA) methodology. We have also implemented an Information Security Governance Process that engages senior management in shaping and driving security strategy.

KLDiscovery's Security Governance Program is backed by global certifications and ongoing compliance initiatives, including:

- ISO 27001 certifications at KLDiscovery Data Centers in the U.S., U.K., Germany, Poland, and Norway
- TIXAS labels for information security and data privacy across 18 locations in North America, EMEA, and APAC
- Annual SOC 2 Type II audits conducted by certified external firms
- PCI DSS Certification for secure handling of payment card data
- U.K. Cyber Essentials Certification for baseline security controls
- HIPAA and HITECH audits ensuring healthcare data protection standards
- FISMA audits supporting U.S. federal information security compliance
- GDPR compliance integrated across applicable global operations
- OWASP-aligned security practices for secure software development

Our Global Commitment to Security Excellence

At KLDiscovery, information security is a continuous pursuit of excellence deeply embedded in every part of our operations. Every safeguard we implement, every process we refine, and every threat we anticipate reflects our dedication to protecting what matters most to our clients.

Our global team stands united by a single principle: trust must be earned and protected every day. We remain committed to delivering security programs that meet today's demands and anticipate tomorrow's challenges, staying with our clients until the job is done right.