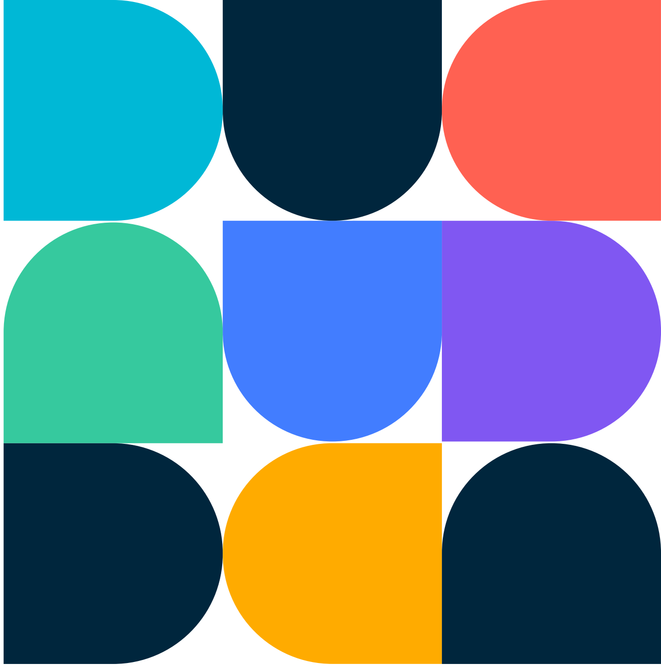
DataBank
A KYOCERA GROUP COMPANY



Information Security management

Multi-layered defense to protect your organization's most valuable data

Trusted security for over a decade

We've developed and maintained a mature Information Security Management System (ISMS), holding an ISO 27001 certificate since 2012 and a SOC 2 compliance attestation since 2010.

Supporting these security frameworks is a year-round commitment with full-time staff as well as multiple third-party and client audits.

Our strengths in controls have been noted by auditors – including:

- Performance monitoring & KPI's
- Communication planning
- Vendor management
- Security awareness training

Flexible to your requirements

We can work within our existing framework, or we can map our existing controls to just about any other information security framework. We've maintained compliance in frameworks like NIST, HIPAA, and HITRUST, and even custom compliance programs developed by clients like you.

Security beyond the checkbox

We don't chase check boxes. We pride ourselves on making evolutionary changes to our systems, policies, and procedures that keep you safe and follow the ever-changing landscape of information security.

Our multi-layered security framework

First layer

Managed Endpoint Security and Network/Systems

Second layer

Active Threat Monitoring - 24/7/365

- Managed SIEM & Threat Intelligence
- Network Behavioral Analysis
- Intrusion Detection & Prevention
- Advanced Persistent Threat Management
- Email Protection Services

Third layer

Policies and procedures

Managed Security: Endpoint and Network/Systems

First layer

Human oversight - Information Security team

We deploy an in-depth, layered approach to data and systems management and protection, leveraging many enterprise level tools and services. Our tools and services have been carefully selected to provide an appropriate amount of overlap and interoperability with independent, 24/7/365 Managed Security Operations Centers at both the endpoint level and at the network/systems level.

Active Threat Monitoring

Second layer

Proactive Defense

Active Threat Monitoring includes, firewalls, routers, and switches, all reporting into our main Security Operations Center and our Security Information and Event Management system (SOC/SIEM). This allows the 24/7 SOC/SIEM to put a massive amount of information from many different touchpoints through AI algorithms and quickly identify areas of concern in the threat surface for the SOC to investigate.

The SOC can then choose to notify Information Security based on criticality/severity or for security orchestration automation and response (SOAR) actions to be taken; such as a ransomware event to be stopped early in the killchain. DataBank is at the forefront in the latest technologies surrounding the detection and response to security threats.

Managed SIEM & Threat Intelligence

With increased regulatory and compliance requirements to combat the escalating number of cyber attacks, we use Managed Threat Intelligence (MTI) for 24/7 monitoring, alerts, and reporting to protect DataBank's IT infrastructure and systems, including your data.

Intrusion Detection & Prevention

Deep-packet network traffic inspections are active 24/7, as well as tunable signatures to ensure vital information is always protected.

Network Behavioral Analysis

Over 1,000 algorithms continuously learn normal network behaviors for a real-time analysis of all inbound and outbound traffic.

Advanced Persistent Threat Management

Advanced analysis and machine learning distinguish normal behavior from abnormal behavior, detecting threats before they cause harm.

Email Protection Services

We use Email Protection Services to guard against threats like ransomware, phishing, fraud and data loss prevention

Policies and procedures

Third layer

Our security fabric

Our final layer is a mature program of policies and procedures including least privileged models, personal device exclusions enforced with technical safeguards, phishing testing, monitoring and limitations on internet access. We pay close attention to all regulatory compliance that comes part and parcel with information security.