daxko®

Data Security at Daxko

Policies. Practices. Technology. Culture.

Abstract:

Your organization owns and controls your data. As your partner and the steward of your data, Daxko is responsible for its security. It's a duty we take very seriously. This paper discusses the many ways we go about protecting your data from threats. It covers specific countermeasures, as well as how we build security into our product development processes and our organization itself. We also address the best practices you should employ to protect your data.

Introduction

Daxko takes the security of customer data very seriously. Our guiding principle is that your data is your data, but we safeguard it. Our goal is to be a good steward of what is arguably your most valuable asset, applying policies, practices, and technology to provide robust protection for your data and doing everything we can to deliver a stable environment with business continuity.

As a SaaS organization, we understand the challenges you face in keeping up with the ever-changing landscape of information security and compliance. Daxko is committed to data security and compliance in all its incarnations. For us, this is about more than just protecting your data when it's part of the Daxko application. Data security is part of our culture and corporate practices spanning product design and incident response. Secure design principles drive our engineering processes and inform our system architecture.

Our overall goal is to give you confidence in our adherence to rigorous security policies, industry standards, and regulatory compliance rules. The results of our efforts include fewer security incidents and security-related disruptions for you, along with better compliance. Our approach gives you the headspace to focus on your operations with the confidence that Daxko is doing its utmost to keep your data secure.

This paper explores how we approach data security, and how it informs our product design process and organization. We'll start with an overview of how we manage information security governance, then delve into Daxko's risk management and compliance practices. We'll cover our information security program, along with how we handle security incidents and address the issue of data ownership. You have a role to play in your data security, too, so we'll share best practices you should implement to protect your data.

Information Security Governance at Daxko

Daxko approaches Information Security with a collection of policies, practices, and organizational units that protect your data and the applications that use it, all while minimizing security-related disruptions.

It all starts with information security governance policies. Our goal is to define and enforce policies that align Daxko software with industry best practices. These include the secure storage, management, and transmission of data, as well as processes like authentication. Our governance policies also deal with systems logging and reviewing third-party vendors.

Governance policies impact employee roles and responsibilities as well, along with employee equipment and acceptable use. Any person or device that touches your data is subject to information security governance policies. This includes system configuration, comprising virus scanning, file integrity monitoring (FIM), the hardening of systems and endpoints, as well as patch management. Incident response processes are also defined through governance policies.

Daxko establishes and executes procedures to support the integrity of production changes—a significant source of risk exposure if not managed according to strict policies. For example, policies address appropriate authorization for releasing new code into production. Any production change needs to be subject to policies like least privilege access and separation of duties (SoD). All changes require an audit trail and must conform to our policy-based software development lifecycle (SDLC).

Who's responsible for carrying out these policies? Daxko's security team defines governance policy and enforcemes it in two units: Compliance and Information Security.

The Daxko Compliance Team maintains data security policies and controls. For example, we have a policy of always encrypting sensitive data such as credit card numbers at rest, which is required for compliance with Payment Card Industry Data Security Standards (PCI-DSS). The Compliance Team enforces the encryption policy in every instance where we store your data.

The Daxko Compliance Team also oversees risk assessments and audits internal systems for policy adherence. This involves mapping policies to system settings for Daxko policies, as well as supporting assessments for System and Organization Controls (SOC 1 Type II) compliance and PCI-DSS. The team further reviews and supports privacy policies, both for internal adherence as well as compliance with regulations such as the California Consumer Privacy Act (CCPA).

The Daxko Information Security Team performs tasks like monitoring system logs and scanning code, along with infrastructure, for vulnerabilities. Team members review infrastructure for misconfigurations which can expose your data to risk. The team further bolsters our security posture by reviewing our architectural practices.

The team works to align security policies with business objectives, collaborating with other Daxko teams to provide guidance on best practices. The process, which includes risk assessments, prioritizes security initiatives and assures policy compliance. Stakeholders use metrics and scorecards to track progress on the status of security projects and the level of risk facing different areas of the business. The team conducts training and promotes awareness across Daxko as well.

Information Risk Management and Compliance

Navigating the intricate web of laws and regulations can be overwhelming, especially when it comes to maintaining compliance with standards like PCI-DSS, SOC 1 Type II rules, and privacy laws like the California Consumer Privacy Act (CCPA). That's where we step in to alleviate some of that burden. Daxko's compliance frameworks are designed to establish robust security measures and safeguard your data while maintaining compliance.

Our team works diligently to ensure that Daxko software remains in full compliance with these regulations, constantly monitoring and adapting to any updates or changes. By partnering with us, you can trust that your organization's information security and compliance needs are being handled effectively, allowing you to focus on other critical aspects of your operation.

PCI-DSS

PCI-DSS is a set of security standards established by major payment card brands (e.g., Visa and Mastercard, etc.). PCI-DSS standards are designed to protect cardholder data and ensure secure payment card transactions. Compliance with PCI-DSS ensures that fitness organizations handle payment card data securely.

PCI-DSS compliance safeguards customer trust and protects their payment information. By following PCI-DSS guidelines, your organization can demonstrate your commitment to data security and build a stronger relationship with your community. Non-compliance can result in fines, legal repercussions, reputational damage, and loss of customers.

Daxko software ensures PCI-DSS compliance, relieving the burden of security management for organizations like yours. To achieve PCI-DSS compliance, Daxko undergoes an annual Third-Party Assessor Review. This rigorous process ensures that our security measures meet the highest industry standards and provides an unbiased evaluation of our adherence to PCI-DSS requirements.

PCI-DSS's stringent requirements protect payment card data:

- Encryption of cardholder information during transmission and storage.
- Implementation of firewalls and access controls to secure network
- Regular monitoring, testing, and updating of security systems
- Strict control measures for employee access to sensitive data.
- Adoption of robust security policies and procedures.

"Daxko's guiding principle is that your data is your data, but we safeguard it. Our goal is to be a good steward of what is arguably your most valuable asset."

SOC 1 Type II Compliance

SOC 1 Type II is an auditing standard developed by the American Institute of Certified Public Accountants (AICPA). It evaluates the effectiveness of an organization's internal controls over financial reporting. SOC 1 Type II compliance ensures the existence of reliable and secure operational controls. It assesses the accuracy, completeness, and integrity of financial data. Compliance also validates that controls are designed and operating effectively to mitigate financial risks.

SOC 1 Type II compliance is important for any organization that handles financial transactions and relies on accurate financial reporting. SOC 1 Type II compliance ensures the reliability of financial controls and data integrity. It assures your customers and stakeholders that proper controls are in place to mitigate financial risks. Non-compliance can lead to financial misstatements, reputational damage, and loss of customer trust.

Benefits of SOC Type II Compliance:

- **Demonstrates a commitment to data integrity, accuracy, and operational excellence.**
- **Assures customers and stakeholders of reliable financial reporting.**
- **Reduces the risk of financial errors and misstatements within the organization.**
- **Enhances trust, credibility, and confidence in the financial systems of fitness organizations.**

"By partnering with us, you can trust that your organization's information security and compliance needs are being handled effectively, allowing you to focus on other critical aspects of your operation."

Software System Security Architecture at Daxko

Effective data security doesn't just happen. It takes dedication and hard work. Daxko follows the best practice of embedding security into our software architecture using security design principles. Our security design principles are extensive, covering a range of functional requirements. Customers find this approach helpful as they grapple with advances in software development and new tools like AI. Daxko's experts keep on top of security practices and build them into our way of designing and protecting our systems.

For example, as we design and develop our applications, we always proceed from the concept of least privilege access. For any functional area of the application, we'll restrict access to all but those users who need it before we even write a line of code. That's the essence of security design principles.

Core elements of our security architecture include:

- **Building in durable, detailed logging from our systems**—This helps with threat detection and security forensics if there's an incident. Session management is a further countermeasure we build into our systems. We design our applications so we can monitor user activity and flag suspicious activity. This means establishing parameters for reasonable timeouts, but also creating methods of identifying users and detecting session hijacking.
- **Applying security design principles after we've identified sensitive data that requires encryption while it's in transit**—This supports **data security and data privacy**. For example, personal identifiable information (PII) should be encrypted in transit to best protect consumer data covered by privacy regulations. It also reduces the liability and cost of handling a data breach. The same goes for storage, where we encrypt sensitive data at rest. The team strives to stay up to date on the most current encryption methods. We also follow the best practice of rotating encryption keys.
- **Conducting data validation**, another area of built-in risk mitigation for your data—Our architecture contains web application firewalls (WAFs), which protect our applications from malicious actors. Among other controls, our data validation methods include detection and alerts for cross-site scripting (XSS) injection attacks, SQL injections, overflow attempts, and unexpected inputs.
- **Designing security into our network architecture**—By segmenting our network, we reduce the risk of an attacker moving laterally across our network. This helps protect your data from breach. Our security design principles also include redundancy, backup, and recovery that provide availability disaster recovery and business continuity.
- **Implementing these principles in numerous practical workflows**—For instance, we regularly update and patch Daxko's systems. We conduct monthly internal scans against all assets and scan for external vulnerabilities against publicly accessible IP addresses.
- **Keeping up with the latest secure development practices**—This allows our team to catch security issues earlier in the development life cycle than was previously possible and remediate them quickly. To this end, we embed threat modeling into the SDLC and conduct code reviews, while also engaging in code scanning and static application security testing (SAST).
- **Incorporating the monitoring of security feeds for new zero-day threats**—Our day-to-day security operations (SecOps) workflows prioritize critical threats for remediation. We complement these practices by engaging an external firm to conduct penetration and segmentation testing. We stay on top of these workflows and overall practices with bi-weekly security reviews between engineering and security teams. The teams review the state of security, answer questions, and track our progress against initiatives.

Information Security Program Development and Management

One of Daxko's primary objectives in data security is to give you the peace of mind that comes from knowing your data is protected by a continually improving security program. It's part of our organizational commitment to data security to ensure our program meets that standard.

Our Security Program consists of the following elements:

- **Continuous education**—As an organization, we stay on top of industry trends and best practices, including the impact of artificial intelligence (AI), emerging threats, and risk management. All employees are required to pass information security training and we supplement that training with routine, company-wide communications. For example, during cyber security awareness month in October we provide training exercises for our teams. These include coding exercises that make them aware of common security vulnerabilities, examinations of the anatomy of attacks that have occurred at other organizations, and deep dives on managing risk.
- **Technology to scale our data security capabilities**—While complexity is growing, we're leveraging automation to scale our security team and increase our responsiveness. We do this by automating our security systems, improving threat detection and response, and expanding the scope of the security data we can review. We're also automating our compliance activities (e.g., detecting new infrastructure and digital assets, and shortening the feedback cycle regarding systems that fall out of compliance or policy).
- **Risk based prioritization**—Everything we do in data security is guided by the level of risk and potential business impact associated with a given threat. By taking this approach, we can do the most to mitigate the most serious risks.
- **A partnership with our technology teams and our customers**—We can only achieve a robust security posture in our products if we build a close partnership between you and the Daxko teams working across security, compliance, and technology engineering. This collaboration leads us to embrace technologies like containers, which enable desired software characteristics as well as security benefits. We also work together to review roadmaps, with the goal of continuously updating technology that's falling out of support, and therefore becoming vulnerable. We also strive to standardize our infrastructure for the sake of security, focusing on hardening, monitoring, and patching.

"As an organization, we stay on top of industry trends and best practices, including the impact of artificial intelligence (AI), emerging threats, and risk management."

Information Security Incident Management

What happens if there's a problem? Information security incidents will occur. That's a fact of life in today's cyber threat environment. Daxko's goal is to quickly resolve security incidents, doing as much as possible to minimize their impact on your organization.

The first, and arguably most important step in security incident response is to be aware that there has, in fact, been an incident. False positives are a problem, but so are stealth attacks that go undetected. We strive to avoid both scenarios by working with an external managed detection and response (MDR) provider that monitors our infrastructure and application for intrusions on a 24/7 basis. This service tracks activity across firewalls, ingress, systems, and web application firewalls (WAFs). Our provider constantly watches our files, looking for unintended changes to sensitive system configurations and alerting our team when they notice a potential problem.

If there's an incident, our teams follow well-defined procedures based on industry best practices for containing threats and escalating the incident if required. Our incident response workflows also include notification responsibilities for customers and legal authorities, when necessary. We back these procedures up with annual training and reviews with senior leadership.

Our incident response processes also incorporate strategies for mitigating the impact of an attack. We block traffic that matches known threat signatures, such as injection attempts, bad networks or bad actors, unfriendly security scans, and suspicious locations. We send our security logs offsite for investigation, working with third parties and relevant legal authorities for forensic analysis of attacks.

"Data security is foundational to our culture and corporate practices. It's embedded in our product design, as well as our security operations workflows and incident response processes."

Your Data Ownership and Daxko's Stewardship

You own your data. That's a bedrock principle for us. We serve as the stewards of your data as it relates to the Daxko applications. This means you have control over your data, and Daxko provides you easy access to retrieve it whenever you need it.

You can access exportable data through the reports provided within each product. These reports are updated at frequencies determined by the product team based on the primary use case of each report. Export options typically include .pdf and .csv options so you can arrange, combine, and edit the data to suit your needs.

In addition to these standard reports, we also offer enhanced reporting options for some products, should you need more flexibility from the data set.

Performance Analytics—From the board room to the fitness floor, empower your leaders and decision makers to track and visualize trends at your organization on the go. Keep a pulse of your organization's health and gauge how you're tracking over time by leveraging our robust and trustworthy industry data.

Daxko Dashboards—Visualize the story in your data with less report pulling and more trend watching. Daxko Dashboards provide an interactive way to see the data you check every day within Daxko Operations. You'll know how your units, members, and account Entries are changing with the touch of a button.

Daxko Vault—Access a database hosted on the Amazon Redshift platform that contains your data produced from your Daxko portfolio of solutions. Daxko users who wish to utilize Daxko Vault will be provided with a username and password that allows you to directly connect to the Amazon Redshift database with any tool supporting PostgreSQL. Your Daxko Vault is designed with analytics in mind. It follows the star schema design pattern defined in the Kimball methodology. This design pattern benefits from the columnar storage architecture of Amazon Redshift. All of these factors together create a powerful analytics environment.

Daxko Exchange—You need connections between your membership management system and other vital software tools your organization leverages. With the Daxko Exchange, you can select from a wide variety of trusted Daxko partners for integrated solutions. Daxko works with each partner to ensure that your data is shared appropriately and safely through our secure API gateway.

Your Data Goes with You Securely—Daxko's Information Security Team operates with the utmost integrity to ensure every step of data extraction is within Security & Compliance. This is for the safety of your organization, our team members, and most importantly your members. Data being transferred is a combination of customer data and consumer PII. Safeguarding and securely moving the data must be done to the highest standards of protection. Daxko provides exiting customers secure Billing Data Extraction as part of their data migration.. This data folder includes detokenized billing data, member photos, signatures, and secure documents. Data is carefully extracted, encrypted, and housed in a secure and password-protected FTP site for **2 weeks**. The Retention Team members guide customers through accessing and downloading data from the secure site.

Empowering Your Chosen Partners with Data Access While You're in Control

Daxko takes pride in delivering a safe and secure partner ecosystem. Over the years, we've built a partnership program, Daxko Exchange, with 3rd party providers who seek to meet your organization's needs. To provide a great experience, we've developed an API gateway that enables your chosen partners to safely and securely access data specific to your organization.

Here are a few things we do to bring you a best-in-class experience while protecting the data:

First, securing your data begins with the vetting of Daxko Exchange partners. New vendors are constantly asking us if they can join the Daxko partnership program. To ensure your data is safe, we only accept partners who will adhere to our data sharing standards. If the partner isn't willing to meet these standards, or if we believe they'll use the data in a nefarious manner, we won't add them as a partner.

Second, we have created an API gateway that all Daxko Exchange partners are required to integrate with if they're going to access your data. This robust gateway gives partners the freedom to build a first-class integration while giving Daxko the ability to monitor and limit what data is being accessed. When building out an integration, we can limit which endpoints a partner is allowed to consume. We monitor when and how frequently they access your data, and we're able to limit how quickly they pull your data to ensure they don't bring down your system.

The gateway is an incredible tool that benefits everyone, and to make sure it does what it's supposed to do we put all our partners through one final review before they're allowed to go live with you. This review gives us one more chance to make sure the data they're accessing pertains to the integration they've built, and again that they're accessing the data safely.

Third, our commitment to security continues with the fact that we won't share data with a partner until you've given Daxko written permission that grants that partner access to your data. We do this by having both you and the partner sign an agreement that grants the partner access to the data while preventing them from sharing or selling the data once they've received it. Only then will we provide the partner with a key that can be used to enable the integration.

"Your data is your data, so you're in control."

Finally, we believe transparency is critical to a successful partnership program. To provide greater transparency we've created a portal where you can see all Daxko Exchange partners, which partners are currently integrated with your organization, and additional information about each partner, including what they do and the specific endpoints they're accessing. If you have concerns about a partner that's integrated with your organization, please reach out to our customer support team. We'll address your concerns appropriately, and if necessary, we can further limit the data partners are accessing.

Your Role in Data Security

You have a critical role to play in your data security. It's wise to invest some time and resources into making sure that your internal systems and devices are secure, and that your team members know what to do to keep your data secure. To this end, we partner with you to support your role in data security.

We advise you to implement internal security practices because many common threats to your data target you, at your location, even if your data is with us. A phishing attack, for example, or an attack that exploits weak passwords or insecure workstations, puts your data at risk regardless of where it's stored. A former employee whose access hasn't been revoked poses a similar threat. Once inside your network, an attacker is well positioned to gain unauthorized access to your data.

For example, once a malicious actor has compromised a user's device (i.e., an endpoint), they can use Daxko software and take screenshots, record screen activity, or log keystrokes to get access to sensitive data. Similarly, an attacker could take advantage of weak passwords or password sharing to breach data stored with Daxko, or commit fraud or identity theft.

Other risk scenarios include the impact of sharing passwords across systems. In this case, an attacker could breach your data by compromising a third party. A breach of your email system could have comparable consequences (e.g., enabling an attacker to impersonate an employee and request a password reset in a phishing attack). Former employees can pose a threat as well if their system access isn't terminated when they leave their jobs.

Daxko Recommended Customer Data Security Best Practices

Passwords

- Use strong passwords
- Do not share passwords across systems
- Use MFA when you can
- Do not use shared logins amongst staff to ensure activity can be traced to an individual

Secure Workstations

- Ensure workstations are locked when staff member is not present
- Access to workstations is authorized, and avoid administrative logins
- Virus Scanning
- Regular system updates enforced
- Update web browser regularly
- Be careful of what browser extensions are used, e.g., those that scan your activity
- Do not install software from untrusted sources

Put policies in place to set expectations with your staff around acceptable use of systems. Ensure access is reviewed for all employees.

- Change access when roles are changed
- Revoke access in a timely fashion when employees are terminated

Best Practices to Keep Your Data Secure: CIO Advice

Managing your employees' access rights is a crucial aspect of ensuring your platform's security. You should grant, monitor, and revoke access as needed, based on their roles and responsibilities. The Y of Central Maryland has shared some best practices around access rights and data security that you can follow to improve your employee access management:

- **Hiring Education**—Before granting access to new employees, ensure that they've completed the necessary platform training for security. This training should cover topics such as password policies, encryption methods, data protection regulations, and incident response procedures. By educating your employees on security best practices, you can increase their awareness and compliance, and reduce the chances of human errors or negligence.
- **Separation of Childcare from Front Desk Activities**—If your organization provides childcare services, separate these activities from your front desk operations. This means that the staff who handle childcare shouldn't have access to the same systems as the staff who handle front desk duties. This simplifies front desk tasks, billing and data risk. Ensure the childcare area is physically secured and monitored to prevent any unauthorized entry or exit that could expose your facility to data risk.
- **Termed Employee Access**—When an employee leaves your organization, immediately remove all their system access, including login credentials, email accounts, cloud storage, and any other resources that they may have used. This will prevent any unauthorized or malicious access by former employees, as well as reduce the risk of data breaches and leaks. When available, review the access logs of termed employees to ensure that they didn't compromise any sensitive information before their departure.

"By educating your employees on security best practices, you can increase their awareness and compliance, and reduce the chances of human errors or negligence."

Conclusion

Daxko is committed to protecting your data, starting with information security governance. We define and enforce policies across our product lifecycle in keeping with PCI-DSS and SOC standards where appropriate. Data security is foundational to our culture and corporate practices. It's embedded in our product design, as well as our security operations workflows and incident response processes. Our commitment extends to our software system security architecture, our information security program, and our incident response workflows.

You have a role to play in your data security, too. Effective data security is based on partnership and mutual support. We recommend following best practices like strong passwords and strict access controls. Working together, we can deliver a reliable, secure service that supports your organization.