# Security Policies

**Device Protection**

In order to protect our internal devices, we utilize Xpertechs.  Mobile devices are not utilized.

**Identity and Access Control**

Robert Isaacs (CEO) is responsible for cybersecurity within the organization.

**Authentication Techniques and Monitoring**

The company utilizes two-factor authentication on all services, as well as Cloudflare “Zero-Trust” security.

**IT Security Staff Experience**

Our IT staff has several years of experience running Cloud infrastructure at large enterprises.

**IT and Security Function Outsourcing**

We use Cloudflare and AWS for web application firewall services.

**Environment Updates**

We follow a monthly update cycle by applying patches to our server software.

**Cybersecurity Event Network Monitoring**

We use Cloudflare monitoring/Palo Alto firewall to monitor our network and alert us to cybersecurity events.

**Unauthorized Access Prevention**

To prevent any unauthorized personnel, connections, devices, and software, we maintain strict physical security, a small office space, and closely trusted staff.

**Inventory for Authorized and Unauthorized Devices/Software**

In order to inventory authorized and unauthorized devices and software, our services are built via automated infrastructure into containers that are frequently recycled.

**Ensuring Timely Installation of Web Application Security Patches**

Every container build updates services and dependencies. Servers themselves run a minimal software stack.

**Preventing Man-in-the-Middle Attacks**

Our application has a valid SSL certificate to prevent “man-in-the-middle” attacks.

**Software Security Assessment**

We assess the security of the software that we develop and acquire via best practices, internal training, and code review.

**Information Processing**

Our organization may process personally identifiable information (PII) or protected health information (PHI) if the MSP ticket data contains those details.

**Third-Party Access to Sensitive Data**

We do not provide third-party access to sensitive data at all.

**Data Classification Security Measures**

We assume customer data is the highest classification (PII info) for the highest level of protection.

**Minimal Level of Personal Information Collection**

We ensure that only the minimal level of required personal information is collected and processed. Additionally, we only permit access to select development staff to work on the service.

**Data Anonymization**

For customers who opt into information sharing, we instantly anonymize the data that is shared with us.

**Backups**

We store containers offsite, and our data is backed up to encrypted local and cloud s3.

**Backup Retention Policies**

We store each customer's backup in a separate area that can be independently recycled. Most data is stored indefinitely.

**Data Recovery Capability**

We restore data from S3 backup sources / services(?).

**Multi-tenancy**

We use the inherent capabilities of data stores to isolate tenants, employing distinct databases where applicable. For files and block objects, individual folders are independently secured. Additionally, separate namespaces are employed for other types of databases.

**Storage of Sensitive Information**

Sensitive information is stored in two places: in our private data center, and in the public cloud in an encrypted S3 AWS bucket.

**Personal Data Transfer Security**

We ensure the security of any personal data transferred between physical devices via private networks.

**On-Site Monitoring**

Our data center is constantly monitored with on-site security. Our office lobby is recorded, and footage is retained for approximately 30 days.

**Dedicated Office**

Our office is not shared with any other entities. Our office space is dedicated solely to Nine Minds.

**Securing Remotely Accessed Sensitive Data**

We ensure that remotely accessed sensitive data (such as data accessed from mobile devices) remains secure through our zero-trust security service (Cloudflare).

**Security Incident Communication**

The process in place to communicate security incidents affecting MSP's data is as follows:

- First, we identify and secure the network using all available resources.
- Next, we work to quickly and accurately identify the scope of the incident.
- Finally, we notify the affected parties.

**Host and Endpoint Security**

We run up-to-date endpoint security, including Defender on Windows and XProtect on Mac OS.

**Network and Infrastructure Security**

Our network equipment is physically secured as our data center is under constant surveillance. We have also equipped on-site security. Access is granted through keycards and codes. Each cabinet is locked.

**Data Center Usage**

The data centers that we use are Hivelocity, Equinix, and Flexential. Two of them store sensitive data. They are all located in the United States and are certified by ISO industry standards.

**Third Party Provider Monitoring**

We monitor our third-party service providers by minimizing our use of third-party providers. Each has a robust policy for notification and includes activated monitoring features.

**Secure Network Infrastructure**

We securely configure our network infrastructure with “zero-trust” remote access to the environment, multiple passwords, encrypted tunnel access, and limited personnel access.

**Network Separation**

The service is not connected to our internal networks at all.

**Blocked and Allowed Communications**

Blocked and allowed communications are stored via web application firewalls.