

At Granite Technology Solutions, we believe strong cybersecurity and proactive IT management are essential to protecting your business, employees, and data.

These standards outline the minimum recommended security requirements. Our goal is to reduce risk, improve operational stability, and help our customers maintain a secure and supported technology environment.

When businesses become managed services customers of Granite Technology Solutions, we work with the business to achieve each of these standards over time.

Granite's Healthy Business Security Standards

At Granite, we believe a customer environment is properly secured when:

- MFA is enabled
- Administrative access is controlled
- Devices are protected and monitored
- Backups are verified
- Patching is active
- Employees receive continuous cybersecurity training
- Security best practices are consistently maintained
- Use of password managers and strong passphrases are consistently enforced

Cybersecurity is not a one-time project — it is an ongoing process that evolves alongside your business.

Identity & Access Security

Multi-Factor Authentication (MFA)

MFA must be enabled for all critical systems and accounts, including:

- Microsoft 365 or Google Business accounts
- VPN access
- Remote access tools
- Administrative accounts for capable systems and hardware
- Preferred MFA method is U2F token or Authenticator app

MFA remains one of the most effective ways to prevent unauthorized access and account compromise.

Account Management Standards

- No shared user accounts
- Separate administrative accounts from daily-use accounts
- No administrator credentials tied to active email “daily driver” accounts
- Administrative access is limited to approved personnel only
- Local administrator rights restricted and documented (when appropriate)

Every user should have unique credentials to improve accountability, security, and auditing.

Endpoint & Network Security

All managed devices should include Granite-approved security protections, including:

- Next-Gen malware protection and Endpoint Detection & Response (EDR)
- Active monitoring and alerting
- Security patch management
- Firewall protection and network security services
- Email filtering and anti-phishing protection
- Email domain security

Preferably, only managed and protected devices should connect to the secure business network. Personal or unmanaged devices should remain on guest or non-secure networks whenever possible.

Backup, Data Management & Patching

Businesses should maintain:

- Verified backups of critical systems and data
- Regular operating system and firmware updates
- Timely application of security patches
- Documented data retention and access control procedures

Unsupported or unpatched systems create significant operational and cybersecurity risk.

Hardware Lifecycle Standards

To maintain security, reliability, and vendor support, Granite recommends the following hardware replacement timelines:

Device Type	Recommended Lifecycle
Laptops	3-4 Years or End of Support
Desktop Computers	4-5 Years or End of Support
Servers	5-7 Years or End of Support
Network Equipment	5-7 Years or End of Support
Backup Equipment	5-7 Years or End of Support
UPS and Battery Backups	7-10 Years for UPS; Battery Backup is model dependent

Proactive lifecycle management helps prevent downtime, improve performance, and reduce security vulnerabilities.



GRANITE
TECHNOLOGY SOLUTIONS

Granite's Healthy Business SECURITY STANDARDS

Security Awareness & Business Protection

Granite strongly recommends ongoing cybersecurity education for all employees through:

- Monthly or quarterly security awareness training
- Phishing simulation testing
- Password security education
- Company security policies and procedures

Additional recommended protections include:

- Password managers
- Cybersecurity insurance
- Ticket approval workflows
- Documented security policies and SOPs, reviewed annually

Recommended Advanced Security Standards

Once minimum standards are in place, Granite recommends additional layered security protections such as:

- Microsoft Business Premium licensing
- Microsoft Entra ID P1/P2 security features
- Hardware security keys (YubiKeys)
- Advanced email and identity protection
- Ongoing technology road mapping and security reviews
- Routine backup testing and recovery validation

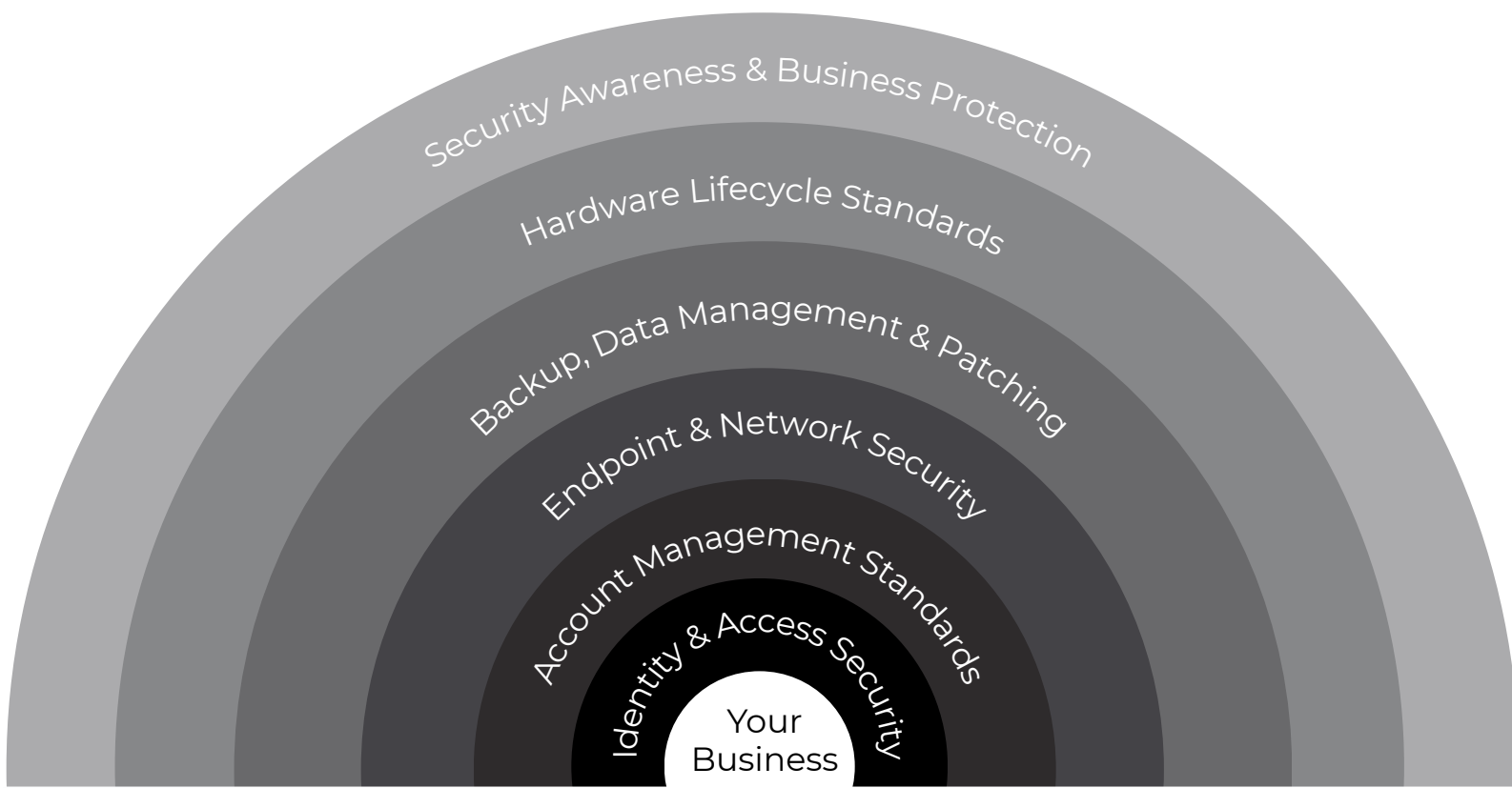
At Granite, we work hard to help each of our managed customers achieve and maintain these protections across their business environments, and we are continuously reviewing security measures, threat prevention tools, and best practices to help businesses stay healthy and secure.



GRANITE
TECHNOLOGY SOLUTIONS

Granite's Healthy Business

SECURITY STANDARDS



HEALTHY USERS

Identity & Access Security

The individual accounts, and devices you are responsible for.

Account Management Standards

The administrative accounts you are responsible for.

HEALTHY ENVIRONMENT

Endpoint & Network Security

The security tools that will detect threats on your devices, email, and other devices on your business network.

Backup, Data Management & Patching

The process to maintain critical routine backups and updates for your software, data, and devices.

HEALTHY BUSINESS

Hardware Lifecycle Standards

The devices in your business environment are within the recommended age for support.

Security Awareness & Business Protection

Participating and completing regularly scheduled and required cybersecurity trainings.



GRANITE
TECHNOLOGY SOLUTIONS

Granite's Healthy Business

SECURITY STANDARDS

Security Standard	Description
Identity & Access Security	Multi-Factor Authentication must be enabled for all critical systems and accounts.
Account Management Standards	No shared user accounts, and limited administrative access. Every user should have unique credentials to improve accountability, security and auditing.
Endpoint & Network Security	All managed devices should include Granite-approved security protections.
Backup, Data Management & Patching	Maintain routine backups and updates. Unsupported or unpatched systems create significant operational and cybersecurity risk.
Hardware Lifecycle Standards	Maintain security, reliability, and vendor support, and keep hardware current by replacing or upgrading equipment.
Security Awareness & Business Protection	Granite strongly recommends ongoing cybersecurity education for all employees through monthly, quarterly, and annual trainings.
Advanced Security Standards (recommended)	Once minimum standards are in place, Granite recommends additional layered security protections such as premium licensing, hardware security keys, and ongoing technology roadmapping.