

Cybersecurity Management



Securing Data is Paramount to Operations

Cyber-threats continue to escalate in both volume and sophistication across today's hyper connected business landscape. GES employs a modern, defense in depth security strategy built on continuous monitoring, rapid threat detection, and adaptive risk mitigation. Our safeguards are engineered to counter a wide spectrum of threats. The cybersecurity program is proactively updated to stay ahead of emerging attack vectors, ensuring all data remains secured, resilient, and protected.

By combining advanced tooling, rigorous security controls, and ongoing threat intelligence, GES works to minimize exposure and maintain a secure operating environment for all stakeholders. Utilizing a robust multi-layered set of cybersecurity solutions and systems our networks are protected with:

- Next generation firewalls at all network perimeter
- Zero trust approach to security requiring authentication to access resources
- Access Control Lists (ACLs)
- Internet content inspection and policy filtering to eliminate unsafe sites
- Multiple layers of Anti-X Filtering Solutions to block malware, spam, viruses, phishing attacks, etc., from entering GES' network
- Internet network access restricted to GES computers only
- All data in transit is fully encrypted
- Multi-factor authentication required for access to all network resources
- Use of intrusion detection and prevention systems
- Advanced Malware Protection (AMP) scanning data flows
- Robust employee security awareness training
- Disaster recovery plan with multi-layered backups both onsite and offsite
- All inbound attachments are sandboxed to verify content safety
- Encrypted corporate file transfer service to send/receive data externally
- Endpoint detection and response (EDR) running on all GES managed devices
- Mechanism allowing staff to report suspected suspicious email activity
- Patch management strategy addressing known vulnerabilities
- Strong password requirements and 30-minute inactivity screen lock-out

2025 Cybercrime Statistics¹

More than 2,300 unique cyber-attacks occur daily

Cybercrime costs worldwide are expected to top \$14 trillion by 2028.

Phishing attacks cost companies an average of \$4.88 million

An estimated 80% of phishing attacks are now AI-generated

7 out of 10 organizations reported more frequent cyber attacks in 2025

GES Cybersecurity Practices and Procedures

Personnel identification and background screening

New employee security training

Monthly cybersecurity training

Subcontractor screening for cybersecurity measures

Controlled behavioral and educational awareness tools

Cyber-asset management

Data loss prevention

Controlled access management

Facility physical hardening

Threat and vulnerability management

Traffic monitoring for malicious content