Genalog

Gills Green Oast, Gills Green, Hawkhurst, Kent. TN18 5ET

PROVIDING SOLUTIONS FOR INDUSTRY

Tel: 01580 753754 Fax: 01580 752979
www.genalog.com email: sales@genalog.com

Genalog Cyber Security Policy

Introduction.

The risk of data theft, scams, and security breaches can have a detrimental impact on a company's systems, technology infrastructure, and reputation. As a result, Genalog has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

Purpose.

The purpose of this policy is to (a) protect Genalog data and infrastructure, (b) outline the protocols and guidelines that govern cyber security measures, (c) define the rules for company and personal use, and (d) list the company's disciplinary process for policy violations.

Scope.

This policy applies to all of Genalog's remote workers, permanent, and part-time employees, contractors, volunteers, suppliers, interns, and/or any individuals with access to the company's electronic systems, information, software, and/or hardware.

Confidential Data.

Genalog defines "confidential data" as:

- Unreleased and classified financial information.
- Customer, supplier, and shareholder information.
- Customer leads and sales-related data.
- Patents, business processes, and/or new technologies.
- Employees' passwords, assignments, and personal information.
- Company contracts and legal records.

Device Security.

Company Use.

To ensure the security of all company-issued devices and information, Genalog employees are required to:

- Keep all company-issued devices, including tablets, computers, and mobile devices, password-protected.
- Secure all relevant devices before leaving their desk.
- Obtain authorization from the Office Manager before removing devices from company premises.
- Refrain from sharing private passwords with coworkers, personal acquaintances, senior personnel, and/or shareholders.
- Regularly update devices with the latest security software.

FM27956

E338838

Certified IPC/WHMA-A-620 Application Specialist

Gills Green Oast, Gills Green, Hawkhurst, Kent. TN18 5ET
Tel: 01580 753754 Fax: 01580 752979
www.genalog.com email: sales@genalog.com

Personal Use.
Genalog recognises that employees may be required to use personal devices to access company systems. To ensure company systems are protected, all employees are required to;

- Keep all devices password-protected.
- Ensure all personal devices used to access company-related systems are password protected.
- Install full-featured antivirus software.
- Regularly upgrade antivirus software.
- Lock all devices if left unattended.
- Ensure all devices are protected at all times.
- Always use secure and private networks.

Email Security.
Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software like worms and bugs. Therefore, Genalog requires all employees to:

- Verify the legitimacy of each email, including the email address and sender name.
- Avoid opening suspicious emails, attachments, and clicking on links.
- Look for any significant grammatical errors.
- Avoid clickbait titles and links.
- Contact the IT department regarding any suspicious emails.

Transferring Data.
Genalog recognises the security risks of transferring confidential data internally and/or externally. To minimize the chances of data theft, we instruct all employees to:

- Refrain from transferring classified information to employees and outside parties.
- Only transfer confidential data over Genalog networks.
- Obtain the necessary authorization from senior management.
- Verify the recipient of the information and ensure they have the appropriate security measures in place.
- Immediately alert the IT department of any breaches, malicious software, and/or scams.

Genalog

PROVIDING SOLUTIONS FOR INDUSTRY

Gills Green Oast, Gills Green, Hawkhurst, Kent. TN18 5ET

Tel: 01580 753754 Fax: 01580 752979

www.genalog.com email: sales@genalog.com

Security software.

To protect our data, systems, users and customers we use the following security systems:

- Laptop and desktop anti-malware and firewall software
- Server anti-malware and firewall software
- Website malware and vulnerability scanning
- Perimeter firewall, Intrusion detection and prevention
- Email anti-malware and anti-spam monitoring and filtering

Backup and disaster recovery.

All Genalog business critical systems are backed up both locally onsite and also externally.

FM27956

E338838

Certified IPC/WHMA-A-620 Application Specialist