Northwestern Mutual Information Security and Privacy Safeguards

The security and privacy of clients’ confidential information are important to Northwestern Mutual. The company takes its responsibility to protect this information seriously and uses technical, administrative, and physical controls to safeguard its data. The following are just some of the ways the company works to keep client information safe.

Technical

Northwestern Mutual uses layers of technical controls to protect its clients’ information:

- **Antivirus** – The company uses antivirus solutions to protect against malicious code that could compromise client information or damage company systems.
- **Email filtering** – The company actively filters incoming email messages for phishing and spam attacks.
- **Encryption** – The company encrypts client information accessed through online account access services to prevent unauthorized users from viewing that information. Company policies require client information stored on mobile devices used for business, including laptops, tablets, and smartphones, to be encrypted as well.
- **Firewalls** – The company uses robust firewall technologies to protect its internal network from unauthorized external parties gaining access.
- **Fraudulent activity monitoring** – The company monitors incoming messages to help identify and prevent fraudulent financial requests.
- **System activity monitoring** – The company uses a variety of resources to monitor systems to identify suspicious activity. Intrusion detection systems and data leakage protection systems reduce the risk of incoming attacks and information loss.
- **Multi-Factor Authentication** – The company provides clients with an extra layer of protection to their northwesternmutual.com account login process by requiring entry of a security code in addition to your user name and password. The security code is a unique, single-use number you receive via phone call, text, or Google’s Authenticator app.
Administrative

Northwestern Mutual supplements its technical controls with processes, procedures, and policies to further protect its clients’ information:

- **Authentication** – The company requires multiple authentication factors to verify the identity of persons requesting policy, contract, or account information. A customer’s right to policy, contract or account information follows state and federal regulations based on their role with the policy, contract or account.
- **Business need to know** – Access to company systems is granted on a business need to know basis. Only those people who need access to a given system and its information to accomplish their job responsibilities receive that access.
- **Change control** – The company uses a change control process to help ensure all changes to company systems maintain the confidentiality, integrity, and availability of those systems.
- **Corporate governance** – The company has a strong governance system with multiple committees supporting information protection initiatives.
- **Cybersecurity threat simulations** – The company conducts cybersecurity threat simulations to identify areas of program strength and opportunities for improvement.
- **Incident response** – The company maintains a well-defined computer security and privacy incident response program, designed to contain and resolve any incidents efficiently and effectively. The program is periodically reviewed and exercised to train and ensure preparation for events.
- **Privacy** – The entire workforce receives information protection training. An Enterprise Privacy team manages the privacy program for the company with the support of contacts across the organization.
- **Internal and external IT auditors** – The company’s internal and external auditors regularly review and assess the company’s information technology systems and operations.
- **Policies and standards** – The company maintains written policies and standards for information protection. These policies and standards provide the foundation and guidance for the company’s information security, privacy, and risk management program.
- **Records management and sanitization** – The company maintains a records management program that manages the lifecycle of the company’s information, including adherence to regulatory requirements and secure disposal of confidential information.
- **Risk assessments** – The company performs risk assessments during the development and acquisition of information systems to help ensure those systems include appropriate protection of client information.
- **Security awareness** – The company recognizes that end users are a critical component of an effective information security and risk management program. The company provides employees and financial representatives with security awareness and training, such as ongoing security awareness articles and events, training in company policies and standards, and simulated phishing exercises. Information to help clients protect themselves is also available on the company’s corporate website, northwesternmutual.com.
- **Separation of duties** – The company separates specific job duties to prevent a conflict of interest when appropriate.
- **Threat monitoring** – The company works with internal teams and third-party industry security organizations to monitor its environment for existing and potential threats.
- **User access reviews** – The company annually reviews user access to company systems to help ensure users maintain an appropriate level of access to those systems.
Physical

Northwestern Mutual also protects its clients’ information from physical harm and theft:

- **Building and data center physical security** – The company controls physical access to its buildings, data centers, and other facilities. Restricted access helps to ensure the confidentiality, integrity, and availability of company systems and physical assets within the company.

- **Business continuity and disaster recovery planning** – The company maintains and periodically tests defined business continuity and disaster recovery plans. These plans are designed to maximize the availability of company systems and information and recover from natural or human-made disasters as efficiently and effectively as possible.

- **Redundancy** – As part of its business continuity and disaster recovery plans, the company maintains redundant data centers to help ensure the availability of company systems and client information.