Information Security Program

Helping protect your financial future is a top priority. We vigilantly monitor the ever-changing world of cyber threats and regularly deploy security enhancements in order to maintain a strong security posture at all times. Our goal is to protect your confidentiality, while maintaining the integrity and availability of all our assets and resources.

Highlights Of Our Information Security Program

Below are some of the measures we take to continually protect and monitor our Information Technology infrastructure and your data:

- **Protecting Your Data:** Our goal is to keep your data safe. Your digital information is encrypted both in transit and at rest to ensure confidentiality. In addition, all sensitive or confidential hardcopy material is securely stored.
- **Multi Factor Authentication ("MFA"):** The process of requiring more than one method of authenticating an account is used both internally and externally. This helps ensure that only intended individuals can access their accounts.
- **Continuous Monitoring & Testing:** Our systems are monitored in realtime to detect any abnormal activity, while also conducting regular penetration testing. In the event any suspicious activity is detected, our highly credentialed security team receives alerts to investigate.
- **Vulnerability Control:** We perform continuous patch management and maintain a vulnerability management program across all systems and employee devices. Our equipment is protected with up-to-date antimalware and anti-virus software.
- **Recovery and Restoration:** In the unlikely event of a security incident or other interruption in our business operations, all of our data storage is in a secured offsite location and we maintain a full disaster recovery and business continuity plan that is periodically tested. These plans are relied on to ensure full enterprise resiliency in order to restore systems to normal operation, confirm that the systems are functioning normally and remediate vulnerabilities to prevent similar incidents.

JOHNSON FINANCIAL GROUP® | BANKING WEALTH INSURANCE

- **Employee Training and Education:** Employees are continually trained on privacy, security and data handling. They are regularly exposed to phishing tests to stay vigilant and to help identify cyber security threats. All employees are required to annually review and signoff that they understand and abide by the company policies on acceptable use, incident handling and code of ethics.
- **Independent Review:** We have independent third-party reviews to ensure the effectiveness of our security practices including processes, policies, procedures and governance activities. These reviews are a means to proactively improve our security program through the identification of any threats or recommendation of best practices.
- **Vendor Management:** We take steps to assess the security posture of all third-party vendors that require access to sensitive or confidential information. These reviews are done internally or through the reliance of an independent Service Organization Control ("SOC") assessment.
- **Regulatory Compliance:** Our security system is in compliance with regulatory requirements from the SEC, FINRA, the Gramm-Leach-Bliley Act (GLBA), The California Consumer Privacy Act (CCPA) as well as any other state breach notification laws or other applicable federal and state laws or regulations.

ADDITIONAL STEPS FOR YOUR OWN PROTECTION

- **Use Strong Passwords and Regularly Update Them:** Always use strong, long and unique passwords for your accounts and avoid reusing a single password across multiple sites. If hackers obtain your password, the first thing they will do is try and use it on other websites. You should also periodically change your passwords and implement Multi-Factor Authentication ("MFA").
- **Avoid Clicking on Suspicious Emails:** Avoid opening links or attachments in an email you are not expecting. Phishing emails will often ask you for personal information in an effort to obtain access to your financial assets and identity. Never respond to emails with sensitive information (like account numbers, passwords, or Social Security numbers).
- **Load Antivirus Software on Your Devices:** Keep viruses, spyware and malware away from your personal files and information by installing antivirus software. Choose one that scans your PC on a regular basis to catch and remove potential threats. In addition, make sure your systems are automatically kept up to date with the latest security patches.
- **Take Precautions at Home:** Safeguard your cell phone or tablet by using a PIN or lock function, download mobile apps with caution, add a strong password to your home WiFi.
- **Don't Share Personal Information:** Don't post personal sensitive information on social media. That includes details such as contact and personally identifiable information. Regularly view your account activity and look out for suspicious transactions. Don't open or accept communications from an unfamiliar source, including phone calls, emails, or texts. Instead, reach out to the individual or company using the contact information from their official website.

Let's start a conversation

For additional information, please contact your Johnson Financial Group Advisor or visit **JohnsonFinancialGroup.com.**