UNITED PLANNERS
FINANCIAL SERVICES

DATA PRIVACY & PROTECTION

WHAT WE DO TO PROTECT CONFIDENTIAL CLIENT INFORMATION

7333 E. DOUBLETREE RANCH ROAD
SUITE 120
SCOTTSDALE, AZ 85258
PHONE: 800-966-8737

Member: FINRA, SIPC

1 COMMITMENT TO DATA PRIVACY AND PROTECTION

In today's digital world, data privacy and protection dominate headlines, from sophisticated cyberattacks against financial institutions to misuse of personal information by global tech companies. Breaches and data leaks are no longer isolated events; they are constant threats in an interconnected ecosystem.

Despite this reality, many organizations continue to rely on templated privacy policies that meet only the minimum regulatory standards, often offering little insight into how your personal or financial information is actually protected.

At United Planners Financial Services, we take a different approach.

We believe that transparency and proactive cybersecurity measures are fundamental to earning and maintaining your trust. That's why we go beyond regulatory requirements to explain exactly how we safeguard your confidential information, not only through policies, but through advanced technologies and secure processes tailored to the modern threat landscape.

From robust encryption protocols and secure networking infrastructure to strict internal access controls and continuous monitoring, our practices reflect a deep commitment to protecting your data in today's complex cyber environment.

2 SECURE AUTHENTICATED COMPUTERS AND MOBILE DEVICES

Laptops, desktops, tablets, and smartphones are all potential attack surfaces in today's threat landscape. If these devices lack proper security controls, such as strong passwords, endpoint protection, encryption, and secure connectivity, they can become entry points for cybercriminals.

Even devices used "just for email" pose significant risk, as email continues to be a primary attack vector for phishing, ransomware, credential harvesting, and other malicious campaigns.

At United Planners Financial Services, we maintain a strict device compliance standard to ensure that any computer or mobile device used to access firm systems, including for communication, meets key cybersecurity benchmarks. While we do not manage these devices directly, we actively audit and enforce the following minimum requirements:

- Strong Passwords: Devices must utilize complex, non-reused passwords and must support automatic lockout features after failed attempts.
- Endpoint Protection: Devices are required to have up-to-date antivirus, anti-malware, and/or endpoint detection and response (EDR) software.
- Operating System & Software Updates: Systems must remain current with all critical security patches and updates installed.
- Encryption: Full-disk encryption must be enabled on all laptops and mobile devices.
- Secure Network Access: Devices must connect via secure, trusted Wi-Fi networks and approved encrypted connections when accessing United Planners' systems.
- Access Verification: When a device attempts to connect to our systems, its compliance posture, including OS version, password hygiene, and connection type, is assessed. If a device does not meet our standards, access may be denied or restricted until the issues are remediated.

Our approach ensures that associates take full responsibility for maintaining secure computing environments, and that we retain the ability to detect, flag, and respond to risks originating from non-compliant devices.

3 SECURE SYSTEMS & NETWORKS AND ONGOING CYBERSECURITY RISK ASSESSMENT

The foundation of cybersecurity at United Planners Financial Services begins with strong technical and administrative controls designed to protect internal systems, applications, and client data. These controls ensure that only authorized individuals can access sensitive information, based on job function, need, and security posture.

But effective cybersecurity isn't a one-time setup, it requires ongoing vigilance, evaluation, and adaptation.

We conduct regular, formalized Cybersecurity Risk Assessments tailored to our unique business model, regulatory environment, and threat landscape. These assessments guide the design and implementation of our controls, ensuring they are current, effective, and aligned with industry best practices.

Unlike firms that outsource core cybersecurity operations, United Planners employs experienced, credentialed cybersecurity professionals on staff who manage and monitor our internal systems and networks directly. This allows for faster response times, tighter control, and deep alignment with our business operations.

To ensure our internal security practices remain robust and transparent, we also engage an independent third-party auditor to regularly assess and validate our cybersecurity controls. These audits verify that our defenses are properly configured, operating as intended, and compliant with applicable regulations and frameworks.

While protecting internal systems is vital, today's business environment requires data to move, between clients, advisors, custodians, and third-party platforms. This introduces a range of risks, especially when data is transmitted over the open internet.

Email, API connections, account aggregation services, and online portals are all potential attack surfaces. Regulatory bodies have highlighted the growing cybersecurity challenges associated with data aggregation and cross-platform sharing.

Traditionally, firms have relied on VPNs, TLS encryption, and secure APIs to protect this data in transit. However, these solutions still operate on the inherently vulnerable public internet, exposing information to interception, latency issues, and access control limitations.

To address this risk, United Planners has adopted a Secure Networking model that enables us to move sensitive data off the open internet entirely.

Through this architecture:

- Only authenticated and authorized parties can participate in the secure network
- Data transmission occurs across a private, segmented, and encrypted infrastructure
- Sensitive information is routed and dispersed over multiple secure channels, significantly reducing exposure to interception
- Performance is faster and more reliable than traditional VPN or internet-based solutions

This private network approach not only enhances security but also supports our vision of a resilient, high-trust digital ecosystem for clients, advisors, and partners.

4 THIRD PARTY VENDOR DUE DILIGENCE

In today's technology-driven advisory landscape, third-party vendors, especially those offering Software-as-a-Service (SaaS), automation, and AI-powered platforms, are foundational to business operations. They deliver convenience, scale, and innovation, but also introduce cybersecurity, privacy, and regulatory risks that can no longer be ignored.

Unfortunately, there are still no universal cyber-

security standards or regulatory oversight for most technology vendors serving the financial services industry. As a result, the burden of due diligence falls squarely on Broker/Dealers (B/Ds) and Registered Investment Advisers (RIAs) to ensure that client data remains protected, no matter where it flows.

At United Planners Financial Services, we embrace that responsibility by maintaining a comprehensive Third-Party Vendor Due Diligence Program, focused on ensuring the security and integrity of client information across all external relationships.

Every vendor is assessed based on the nature of the services provided, access to client or firm data, and potential impact to operational or reputational risk. We review whether vendors follow established cybersecurity frameworks (e.g., NIST CSF, ISO 27001), maintain effective access controls, perform routine penetration testing, and support secure software development practices.

As AI tools become more integrated into vendor offerings, we conduct detailed assessments on how AI models are trained and monitored, safeguards against bias, misuse, and hallucination, data input/output protections, and human oversight.

We also require vendors to demonstrate adherence to all relevant regulatory requirements, including Regulation S-P, Reg BI, FINRA Cybersecurity Guidelines, and federal/state data privacy laws (e.g., GDPR, CCPA/CPRA). Depending on the risk tier, independent security assessments such as SOC 2 Type II or policy documentation may also be required.

While we do not require every vendor to operate within our secure network infrastructure, we proactively establish a Secure Networking environment to enable safer, more controlled communication and data exchange between United Planners, our advisors, and trusted vendors. This ensures sensitive data can be transmitted over authenticated, encrypted, and segmented private pathways, without relying on the open internet.

United Planners requires all associates to complete training and testing to identify their vulnerabilities and strengthen their reaction to potentially dangerous situations such as phishing attacks. The training is designed to address common types of attacks targeted at individuals working in the financial services industry, and provide specific guidance based on how the individual reacted to the test.

5 CYBERSECURITY AWARENESS TRAINING AND TESTING

While secure devices, systems, and networks are critical foundations of any cybersecurity program, technology alone cannot defend against every threat. In today's environment, where phishing emails are increasingly sophisticated and cybercriminals actively exploit human behavior, people, not tools, often represent the first line of defense.

Research continues to show that the majority of cybersecurity incidents stem from human error, such as clicking on malicious links, falling for impersonation attacks, or failing to follow basic data protection protocols. That's why United Planners Financial Services places strong emphasis on proactive, continuous cybersecurity awareness training and testing.

All associates are required to complete annual cybersecurity training that covers the most common threats facing professionals in the financial services industry. This includes topics like phishing recognition, safe document handling, secure communication practices, and device hygiene. The training is updated regularly to reflect new attack patterns and regulatory expectations.

In addition to structured training modules, United Planners conducts routine phishing simulations to reinforce awareness and improve real-time response behaviors. These tests are designed to mirror real-world social engineering tactics, and associates receive individual feedback and coaching based on how they respond. This hands-on approach strengthens our team's ability to spot and report threats before they cause harm.

By investing in our people as part of our cybersecurity strategy, we foster a culture where security awareness becomes second nature, not just during annual training, but every day. Our goal is to empower every associate with the knowledge and instincts to protect sensitive information and act confidently when faced with suspicious or potentially harmful digital activity.

6 INCIDENT RESPONSE PLAN AND CYBERSECURITY INSURANCE

No matter how advanced a cybersecurity program may be, no system is immune to threats. Between increasingly sophisticated cyberattacks, constantly evolving technologies, and the ever-present potential for human error, the risk of a security incident is never zero.

What matters most is how an organization responds when an incident occurs.

At United Planners Financial Services, we have developed and tested a detailed Incident Response Plan (IRP) designed to ensure swift, effective, and compliant handling of data security events. Our plan outlines clear roles, communication protocols, and escalation procedures, so that if a breach were to occur, the response is immediate and coordinated.

Our internal cybersecurity professionals work in tandem with legal, compliance, and external experts to investigate incidents, contain threats, and mitigate impact. From digital forensics to system recovery and client notification, we are prepared to respond with speed and clarity.

As part of this preparedness, United Planners also maintains a comprehensive cybersecurity insurance policy. This policy not only provides financial support in the event of a data breach, but also grants access to specialized external resources, including breach response consultants, forensic investigators, and legal advisors, to ensure full remediation and regulatory compliance.

Importantly, our coverage extends beyond just the home office. United Planners' policy is structured to also include our network of independent contractor financial advisors and their practices, a critical protection layer in today's distributed, advisor-centric model.

This dual focus on proactive response and strong insurance coverage reflects our commitment to protecting not just our systems and data, but our advisors, their clients, and the firm's long-term integrity.

7 CONCLUSION

At United Planners Financial Services, cybersecurity is more than a regulatory obligation, it's a fundamental part of how we earn and maintain trust.

We have taken proactive, deliberate steps to go beyond industry standards in protecting personal and financial information. From secure systems and internal controls to advisor training, third-party due diligence, and incident response preparedness, every layer of our cybersecurity program is built with care, tested for resilience, and verified by independent experts.

We also recognize that cybersecurity is a shared responsibility. That's why we support our financial advisors with the tools, infrastructure, and guidance needed to operate securely in a complex digital environment.

This commitment reflects our broader culture of compliance, one that values transparency, accountability, and continuous improvement. It's how we provide peace of mind in an age of increasing cyber risk and why clients and advisors alike can feel confident doing business with United Planners.

UNITED PLANNERS
FINANCIAL SERVICES

7333 E. DOUBLETREE RANCH ROAD
SUITE 120
SCOTTSDALE, AZ 85258
PHONE: 800-966-8737

Member: FINRA, SIPC

Revised:: 08/25/25