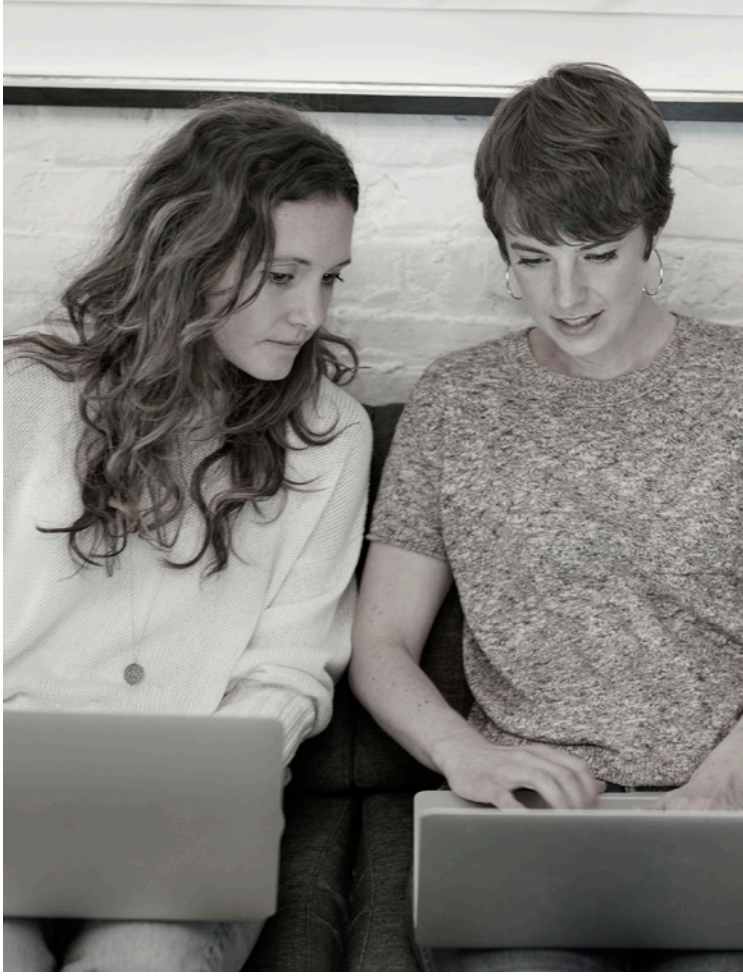
WHITE PAPER

TRINET SECURITY AND PRIVACY

January 2025



TriNet was founded in 1988 and has been delivering industry-leading HR outsourcing services to our customers for more than 30 years.

TriNet guides small and medium-size businesses through their daily HR needs and challenges with passion, empathy, and proven expertise.

Security and privacy play an integral role in the design and structure of our business operations and the services we provide. TriNet is committed to delivering an incredible experience to our customers and meeting their security and privacy expectations, while focusing on ensuring compliance with regulatory requirements.

Our security measures, policies, and standards demonstrate a commitment to maintaining the confidentiality, integrity, and availability of the information entrusted to us by our customers and the approximately 540,000 individuals who use our services.

INFORMATION RISK MANAGEMENT

TriNet's enterprise-wide Information Risk Management (IRM) Program provides a framework for and governance of risk-based management of all TriNet information. The IRM program consists of six core functions:

- **Security:** Identifies, implements, and maintains critical security capabilities to safeguard the confidentiality, integrity, and availability of TriNet information.
- **Privacy:** Responsible for the appropriate collection, protection, use, and disclosure of personal information as governed by relevant laws, rules, and regulations.

- **Third-Party Risk Management:** Provides an understanding of risks associated with sharing TriNet information with third parties and the management of that risk.
- **Data Governance:** Defines the strategy of availability, usability, integrity, and security of data used by TriNet.
- **Records Management:** Defines the desired behavior in the creation, use, retention, and disposition of corporate records.
- **Technology Operations:** Ensures governance and information risk protection requirements are designed, implemented, and executed to achieve IRM objectives.

INFORMATION SECURITY AND PRIVACY FRAMEWORKS

Integrated Risk and Control Framework

TriNet has a robust Integrated Risk and Control Framework (IRCF) that is designed to secure information assets and technology resources from unauthorized disclosure, modification, deletion, and destruction. TriNet's IRCF, modeled on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and Privacy Framework, promotes information security, privacy, and risk management at TriNet.

Furthermore, this framework considers various industry standards, including:

- NIST SP 800-53 Rev. 4, encompassing security and privacy controls;
- Cloud Control Matrix (CCM) v3.0.1;
- COBIT 5, with a focus on Control Objectives for Information and Related Technology;
- CIS Controls from the Center for Internet Security;
- Trust Principals by the American Institute of Certified Public Accountants (AICPA); and
- Health Insurance Portability and Accountability Act (HIPAA).

SECURITY AND PRIVACY STRATEGY AND GOVERNANCE

Security Program

The Chief Security Officer (CSO) provides overall leadership, direction, and guidance for the operation of TriNet's Security Program. The CSO:

- Provides strategic leadership for the program and related information security teams; and
- Prioritizes security initiatives to mitigate risks to TriNet information.

The TriNet Security Program's mission is to enable the success of both TriNet and our customers through a risk-based program to ensure critical assets are safe, resilient, and secure. We are committed to maintaining the confidentiality, integrity, and availability of the information entrusted to us by our customers and colleagues.

Privacy Program

The TriNet Privacy Office (TPO), led by TriNet's Chief Privacy Officer, makes protecting the personal information of our customers, colleagues, and worksite employees (WSEs) their top priority. We believe that everyone should know what we do with their information, who we share it with and why. These tenets are at the center of the TPO's mission and are the strategic cornerstones of the TriNet privacy program. For more information about Privacy at TriNet, please visit: **https://www.trinet.com/privacy**.

Policies, Standards and General Requirements

TriNet maintains and regularly updates a comprehensive catalog of policies and standards which serve as the governance foundation for our privacy and security programs by establishing reasonable and appropriate safeguards for TriNet information, technology resources, and the information entrusted to us by our customers. The policies and standards listed below are reviewed and approved by respective leadership annually:

- Assurance Management Policy;
- Configuration Management Policy;
- Identity and Access Management Policy;
- Information Security Management Policy;
- Mobile Device Policy;
- Operations Management Policy;
- Service Management Policy; and
- Technology Resource Acceptable Use Policy.

In addition, TriNet employs a defense-in-depth approach to protect our network, systems, users, and information against internal and external threats.

We also implement general security requirements that follow industry-based standards:

- Access Control Standard;
- Asset Management Standard;
- Backup and Storage Standard;
- Business Continuity / Disaster Recovery Standard;
- Change and Release Management Standard;
- Cloud Third-Party Risk Management Standard;
- Cryptography Security Standard;
- Information Protection Standard;
- Inventory and Configuration Management Standard;
- Issue Management and Risk Response Standard;
- Network Security Standard;
- Physical Security Technical Design Standard;
- SDLC and Software Acquisition Standard;
- Security and Privacy Incident Management Standard;
- Security Architecture and Secure Builds Standard;
- Security Risk and Compliance Management Standard;
- Security Training and Awareness Standard;
- Software Distribution Standard;
- Third Party Risk Management Standard; and
- Vulnerability Management Standard.

Promoting Security and Privacy Awareness

We believe that to be responsible data stewards our approach to privacy and security awareness must extend beyond the requirements set forth in a particular corporate policy or framework. That is why we invest in privacy and security education and awareness efforts to support a vigilant and mindful workplace culture. On an annual basis, colleagues are required to complete trainings that reflect up-to-date privacy and security requirements, in addition to best practices.

Our annual trainings include courses specific to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the handling of sensitive information. We augment company-wide efforts with targeted training at multiple levels of the company. We conduct in-depth tabletop exercises and role-based technical security training based upon job responsibilities. We have also established a robust phishing training and awareness program that includes monthly phishing tests to increase colleague awareness on identifying and reporting suspicious emails.

TriNet goes beyond required trainings to keep colleagues alert to privacy and security issues in everyday work and life. As part of this effort, the TPO holds an annual Data Privacy Day celebration to highlight current events and simple habits that can have a big impact on how data is handled. The TPO also regularly publishes articles on the TriNet intranet site regarding timely privacy topics.

Our approach to security awareness is similarly engaging and accessible. The TriNet security team promotes Cybersecurity Awareness Month each year with digital signage and video messages from leadership, and hosts engagement activities and competitions. The security team also regularly publishes newsletters and articles highlighting important security best practices while reinforcing an engaged security culture.

INCIDENT MANAGEMENT

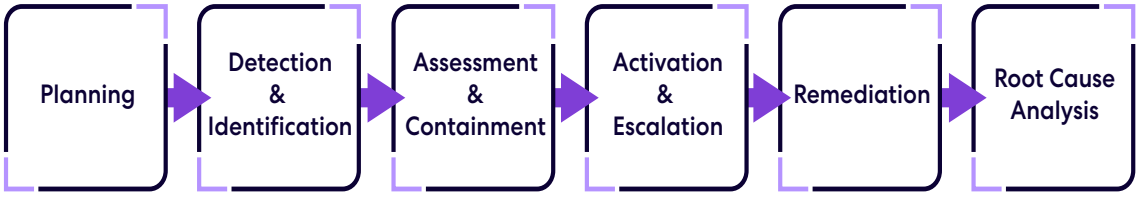
Security Incident Response

TriNet's Security Incident Response Plan is the cornerstone of our cybersecurity strategy, enabling us to respond swiftly and effectively to security incidents while safeguarding the information of both TriNet and our valued customers. Our primary objective is to restore normal service operations promptly and minimize any potential disruption to business operations. TriNet conducts quarterly security tabletop exercises to maintain our readiness, during which we rigorously test our incident response procedures. Additionally, we incorporate proactive threat hunting techniques, ensuring that we remain vigilant in identifying and mitigating potential threats before they escalate.

Privacy Incident Response

TriNet also maintains a documented Privacy Incident Response Plan which governs how we respond to a potential compromise of personal information, such as loss, misuse, or unauthorized access scenarios. Our policy is to promptly contact the authorized customer representative and provide updates as they become available via the assigned service team or point of contact.

Security and Privacy Incident response plans and playbooks are reviewed and updated annually and are aligned to the following process:



PRIVACY BY DESIGN

TriNet integrates respect for individual privacy rights and proactively addresses privacy in the creation and operation of new products, systems, and processes. Our goal is to embed privacy principles as part of the foundation of our products and services. We aim beyond meeting minimum requirements and instead strive for best practices and ethical treatment of the personal information entrusted to us. One of the ways we incorporate privacy by design into our business is by conducting Privacy Impact Assessments (PIAs) to ensure that privacy risks are considered and addressed.

SECURITY BY DESIGN

Security by Design is a core principle of our development process. It means that we consider the security implications of every design decision, from the initial stages of planning to the final stages of testing and deployment. We use industry leading practices and standards such as the OWASP Software Assurance Maturity Model to guide our process to ensure that our products meet the highest levels of confidentiality, integrity, and availability. We also perform static and dynamic application security testing as an early quality gate, provide security training for our developers, conduct regular penetration tests, and maintain a rigorous remediation program. By adopting Security by Design, we aim to deliver software that is secure, reliable, and trustworthy for our customers and their sensitive data.

Secure Software Development Cycle

TriNet utilizes a secure software development lifecycle that includes the following steps to prevent and / or detect security vulnerabilities:

- Dynamic, static, and interactive application security testing;
- Comprehensive application security training curriculum;
- Security findings review;
- Privacy Impact Assessments;
- Mobile application security testing;
- Automated security scans; and
- Security Architecture and Engineering.

TriNet has developed security architecture standards and processes to support secure design and configuration of networks, network infrastructure, and information systems. The program is designed to:

- Analyze enterprise security architecture for deficiencies;
- Determine appropriate security monitoring requirements;
- Determine capabilities to support continuous monitoring of the security of the environment; and
- Measure Security Architecture effectiveness.

IDENTITY AND ACCESS MANAGEMENT

TriNet's Identity and Access Management program improves security through processes and tools to manage user access across all TriNet systems. The program capabilities include:

- Multifactor authentication;
- Centralized access management;
- Access reviews; and
- Defined requirements for privileged access management and segregation of duties.

THIRD PARTY RISK MANAGEMENT

The Third Party Risk Management Program, guided by the Third Party Risk Management Standard, encompasses the following capabilities:

- Maintaining a risk-based inventory of third party vendors;
- Requiring that third party vendors undergo risk-appropriate due diligence before contracting and continuous monitoring afterward;
- Informing the negotiation of contracts with Third Party vendors by ensuring that vendor contracts have the appropriate safeguards in place to protect TriNet information and TriNet systems; and
- Enabling the appropriate disposal or sanitization of TriNet information in the custody of third party vendors.

BUSINESS CONTINUITY, DISASTER RECOVERY, AND CRISIS MANAGEMENT

TriNet's business continuity and disaster recovery capabilities are designed to minimize the loss of customer data and ensure that the TriNet platform and associated services remain available to our customers. TriNet has aligned its Business Continuity Program to adhere to ISO 22301, the international standard for business continuity management.

The Business Continuity Program is designed to:

- Ensure the safety and security of colleagues;
- Provide an understanding of essential procedures, systems, and personnel; and
- Ensure critical processes and essential personnel can continue operations or quickly return to operations after an unexpected outage.

As part of the Business Continuity Program, TriNet has implemented an all-hazards Crisis Management Plan (CMP) and Framework that is meant to engage subject matter experts throughout TriNet in a timely manner at the first awareness of a potential crisis. The Crisis Management Playbook provides a roadmap for how to promptly respond to a crisis—whether it is of a physical or non-physical variety—and transition back to normal business operations.

TriNet servers are replicated using a multi-layered methodology and include one to two levels of redundancy to ensure 24/7 availability of business functions and data in the event of a loss of one or more servers. This methodology helps TriNet maintain continuous system and data access, even if one or more servers fail.

PHYSICAL SECURITY

Physical and environmental security of TriNet facilities and facility locations is foundational to the protection of information assets and technology resources against unauthorized disclosure, modification, deletion, and destruction.

Access to TriNet facilities is restricted to authorized personnel. Physical security measures at TriNet facilities include:

- Centrally controlled door locks and locked windows;
- Reception desks in designated public areas within the facility;
- Electronic physical access control system;
- Access badges for authorized personnel;
- Video surveillance; and
- Physical security and safety incident monitoring and notification system.

TriNet policy requires all visitors to sign in and be escorted by authorized personnel when accessing TriNet facilities.

COMPLIANCE AND AUDIT

TriNet recognizes the importance of maintaining an appropriate internal control environment and reporting method on the effectiveness of its internal controls. TriNet's Internal Audit team conducts reviews throughout the year based on TriNet's risk-based audit plan.

SSAE16/ISAE 3402/SOC2

Service organization control (SOC) reports are independent, third party assessments of our financial, security, and data protection practices.

The American Institute of Certified Public Accountants (AICPA) SOC 2 audit framework defines trust principles and criteria for security, availability, processing integrity, and confidentiality. The SOC 1 report is developed under the AICPA's SSAE16 standard. TriNet has both a SOC 1 Type 2 report and a SOC 2 Type 2 report for the TriNet platform. Current copies and corresponding bridge letters (issued each calendar quarter) are available upon request and are reserved for existing customers.

SARBANES-OXLEY ACT

TriNet continues to invest in improving our internal control environment to support our ongoing compliance with the requirements of the Sarbanes-Oxley Act of 2002 (SOX). All TriNet colleagues play an important part in SOX compliance by being held accountable to the entity level controls that apply to them. TriNet's internal SOC and SOX compliance audit and review process occurs throughout the year, with established planning, review, and testing phases.

STATE PRIVACY LAWS

While privacy laws differ from state to state, and region to region, they generally regulate the collection, use, and sharing of personal information. These laws also provide individuals with specific rights regarding their personal information. TriNet maintains a cross-functional team that monitors state and regional privacy law developments to address any corresponding risks and compliance obligations.

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that established data privacy and security requirements for certain entities that interact with individual's health information. HIPAA mandates privacy and security protections for protected health information (PHI) and applies to individuals and entities that meet the definition of "covered entities" or "business associates" under HIPAA. TriNet maintains a HIPAA compliance framework that monitors and tracks our compliance to the requirements of HIPAA.

About TriNet

TriNet (NYSE: TNET) provides small and medium size businesses (SMBs) with full-service HR solutions tailored by industry. To free SMBs from HR complexities, TriNet offers access to human capital expertise, benefits, risk mitigation and compliance, payroll and real-time technology. From Main Street to Wall Street, TriNet empowers SMBs to focus on what matters most—growing their business.

Go to **TriNet.com** to get started or speak with a TriNet representative at **888.874.6388.**

Learn all about our tailored solutions at TriNet.com or call 888.874.6388.