TP Security and Privacy Program

Table of Contents

Message from the Global Chief Information Security Officer

TP is deeply committed to safeguarding client data and continues to make substantial investments to ensure robust cyber resilience. Our security strategy is designed to identify, defend against, respond to, and recover from even the most advanced cyber threats. Our strategic objectives are to:

- Ensure uninterrupted client service delivery
- Prevent data breaches across client and corporate environments
- Safeguard business processes from compromise
- Detect and prevent fraudulent activity
- Develop secure digital solutions

Our security architecture is built on a layered defense model that integrates identity management, network segmentation, endpoint protection, and continuous monitoring. It is designed to support zero trust principles, ensuring that access is verified at every level. We align our architecture with recognized global standards and frameworks (ISO 27001, ISO 27701, ISO 42001, PCI DSS, HIPAA/HITRUST, NIST Cybersecurity Framework) to maintain resilience, scalability, and compliance across diverse environments. We leverage industry-leading security technologies and maintain a highly skilled information security team. These capabilities are further enhanced by proprietary TP security solutions.

Security is not a one-time achievement—it's an ongoing commitment. TP continuously evaluates and enhances its cybersecurity posture through regular internal assessments, threat intelligence updates, and feedback loops from incident investigations. We proactively adapt to emerging threats and evolving regulatory landscapes, ensuring our defenses remain resilient and our practices stay ahead of industry expectations.

Our frontline defense is our globally trained, cyber-aware workforce. Through a rigorous security awareness and Human Risk Management program, we simulate over 100,000 phishing emails monthly to train employees in threat recognition and response. When active phishing campaigns are detected, we immediately alert staff via our Workforce Management Messaging System with "Be on the Lookout" notifications.

We provide 24/7/365 monitoring and incident response through two follow the sun global Security Operations Centers (SOCs). These SOCs support our four regional Cyber Defense Centers (CDCs). Additionally, our global fraud and incident investigation team operates across seven countries and supports clients in English, Spanish, Portuguese, and local languages in India and the Philippines.

We maintain strict access controls and enforce multifactor authentication for remote access and implement advanced endpoint posture controls. Our endpoint detection and response technologies are designed to prevent ransomware and other high-impact cyber threats. Continuous threat hunting is conducted by our SOCs, our CDCs and an independent third-party service for added vigilance. Elevated privileges require FIDO2-compliant tokens used exclusively from verified TP administrator workstations or Jump Hosts.

Our IT infrastructure undergoes annual independent assessments aligned with ISO 27001, ISO 27701, ISO 42001, PCI DSS, SOC 2 Type I and II, and HIPAA/HITRUST standards.

TPs digital solutions are designed to embed security from the ground up. Integrating identity protection, data privacy, and threat mitigation into every layer of the technology stack. These solutions are built to meet global compliance standards and are tailored to support secure client interactions, resilient operations, and scalable growth in dynamic environments.

TP looks forward to protecting your service delivery, and we are grateful for your business and entrusting your customers' data with our team.

Very Respectfully,

Christian Muus
Global CISO

1. Introduction

For over 40 years of continuous improvement and innovation, TP, has been a trusted global partner in delivering digital business services that connect the world's most successful companies with their customers. As a leader in customer experience management and digital transformation, TP empowers organizations to scale operations, enhance engagement, and drive growth through intelligent, tech-enabled solutions.

TP employs over 500,000 professionals across 100 countries, servicing clients in over 170 territories and communicating in more than 265 dialects. TP is a trusted partner to many of the world's leading brands because our advanced business solutions help them deliver truly integrated, human-centric experiences while optimizing business processes and performance.

TP's commitment to security and trust is embedded in every solution. We continuously evolve our security posture by:

- Adopting cutting-edge technologies
- Monitoring emerging risks and threats
- Complying with international data privacy regulations

TP ensures information security, compliance, and privacy protection for all stakeholders—including employees, suppliers, customers, business partners, clients, and their end users. This is achieved through:

- Industry-leading security policies and standards
- Robust control frameworks
- Ongoing alignment with internal and external market trends

As a digital business services provider, TP remains at the forefront of innovation—transforming customer experiences while safeguarding the integrity of every interaction.

2. Information Security Program Overview

TP is committed to improving information security throughout its organization. It has implemented a deliberately layered series of mechanisms and controls to protect the confidentiality, integrity, and availability of its systems, networks, and data whether in-transit or at-rest. Our information security program is a combination of policies, security architecture, classification of information, risk management processes, incident response plans, security operations, security awareness and training, and monitoring security metrics to assess the achievement of our security objectives.

TP's information security program is geared to protecting the entire business ecosystem: clients, customers, and employees.

The Global Chief Information Security Officer leads TP's information security team. This team includes security governance, risk management, IT security operations, incident response, security engineering, and cyber security management. The team's training programs and certifications demonstrate our proactive approach to keeping up and aware of current threats and technologies to be able to protect our environment. Moreover, the company's regional CISOs oversee the information security program from both a region and subsidiary level.

TP Enhanced Cyber Security Program:

- Zero Trust Network Architecture designed to reduce attack surface area
- White Hat hackers supported by reputed organization
- Multi-layer approach from perimeter to end point including proprietary security technology products
- Established organization-wide security awareness (e.g., anti-phishing)
- Aligned to industry best practices
- End to end detection and response framework

People: extensive cyber security training across TP

- Extensive cybersecurity training in 16 languages completed by 500 000 people
- Dedicated security organization
- C-level Security Governance

Process: security and privacy by design and default, audits, and white hacking

- Security by design, External audits, and Whitehat hacking
- Security Risk Assessment (SRA)
- GISP
- NIST cyber security Framework Alignment

Culture: promoting a cyber-smart culture within the enterprise

- Our employees are our most important security measure
- Promoting a cyber-smart culture within the enterprise

Technology: re-architecting the network; tools to enhance the detection capabilities through Global Security Operation Center

- Detection tools and Global Security Operation Centers
- Virtual Briefing Center
- TP Protect
- TP Patented security monitoring technology

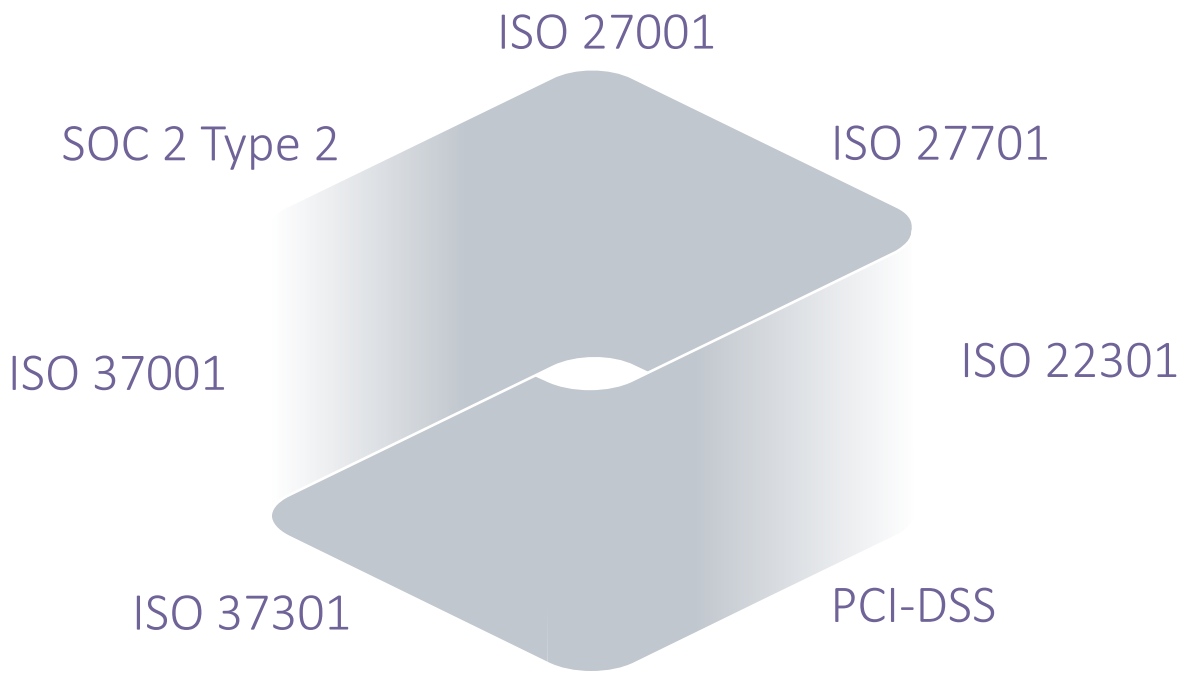
3. *Certifications, Recognitions & Alignments*

TP is the first company in the industry to comply with the Binding Corporate Rules (BCRs) in the European Union. We have BCR status as a controller and processor.

Our clients can trust us with customer data and be assured of receiving the same level of protection in Europe and any other country where we operate.

Certifications

We constantly adapt our technology, monitor risks and threats, comply with international data privacy regulations, and seek new ways to protect company and customer data.



Recognitions

TP leads innovation, delivering cutting-edge services and products.

We are thrilled to announce that TP has been recognized as a winner in the 2025 BIG Innovation Awards in the Innovation-Product category for our microservices and GenAI solutions.

TP's AI-driven digital solution has been recognized as the Gold winner in the 'Best New Product or Service Innovation – Technology' category at the 16th Annual 2024 Golden Bridge Awards®.

TP India has been recognized for 'Best Implementation of Gen AI for Business 2024'.

Alignments

- NIST CSF v2.0
- FISMA
- HIPAA

4. IT, Security and Privacy Charters

Global Compliance and Security Council Charter (GCSC Charter)

The Global Compliance and Security Council (GCSC or the Council) is the TP SE (TP) principal governance body that oversees the implementation and management of TP Information Security Policies and Global Legal, Privacy & Compliance Policies for TP's Core Business units.

The Council, composed of TP Global and Regional senior leadership, is responsible for establishing TP's risk appetite and directing mitigation activities and investments in alignment with the strategic mandates of the TP Board of Directors.

Using a data-driven approach, the Council aims to reduce the overall security and compliance risk exposure of TP's Core Business units.

The GCSC has two sub-committees: The Policy Working Group and the Data Governance Group:

- Policy Working Group (PWG):

  The Policy Working Group is the principal body for reviewing and approving our global policies.

- Data Governance Committee:

  The Data Governance Committee has several Working Groups that support the organization in managing risk in relation specifically to data. These are:

  - AI & Data Innovation Group
  - Health Information Governance Group
  - Records Management Group

Architecture Review Board (ARB)

The Architecture Review Board (ARB) plays a pivotal role in strengthening TP's IT governance and strategic alignment. It serves as a centralized body that ensures architectural consistency, enforces enterprise-wide standards, and promotes transparency across technology domains.

The ARB's core objectives include:

1. Aligning IT initiatives with business strategy by setting architectural policies and guiding principles.
2. Evaluating and approving architectural decisions to ensure scalability, security, and operational efficiency.
3. Filtering solution requests to prioritize strategic initiatives and promote the adoption of effective technologies.
4. Ensuring architectural consistency and compliance by applying standardized design principles and adhering to internal policies and external regulations.

Technology, Privacy and Security Committee Charter (TPSC Charter)

The Technology Privacy and Security Committee (TPSC) is a global governance decision body responsible for reducing risk in relation to proposed projects, and is managed with respect to corporate policy and regulatory compliance, cyber security, data and privacy and technology integration and investments,

including AI. Each TPSC executive is responsible for developing risk assessment questions for their area of responsibility to facilitating risk assessment by the TPSC.

5. Audits

External Audit

An external audit firm annually reviews all corporate controls as part of TP's Information Security Policy and its regulatory certifications. The control review includes, but is not limited to, logical access, physical access, change control, risk assessment, data flow.

Internal Audit

TP auditors review over 200 security and privacy controls regularly to ensure compliance with our security policies and standards. These controls include, but are not limited to, physical access to restricted areas, device admin access and access control, asset management, and security contractual compliance.

Penetration Testing

Annually, a penetration test is performed on all in-scope internal and external facing devices and applications including network layer tests. The testing covers all requirements in the PCI data security standards. Vulnerabilities discovered during penetration testing are appropriately addressed following the standard severity categorization.

Vulnerability Scanning and Assessment

TP has established a regular review process for discovering and mitigating security threats and vulnerabilities. There are two types of vulnerability scans performed--web application scans and network and systems scans. Vulnerability scans are also performed on both internal and external facing devices and applications at least quarterly.

6. Security Risk Assessments

Our Security Risk Assessment is a proactive, non-intrusive method to identify potential risks in processes and applications within the call center environment. A Security Risk Assessment reduces risks for TP's clients and its customers while increasing privacy. The primary goal of a Security Risk Assessment is to help design a strategy to reduce risks and provide methodologies for early detection of unauthorized behavior associated with known risks that cannot otherwise be eliminated.

Examples of what our Security Risk Assessment can discover:

- Unauthorized actions by call center employees using their approved access into client CRM tools, and processes that could lead to a privacy breach or theft.
- Applications or tools that are available to call center employees while not required for their job functions.
- Applications or tools that should not be accessible from a public network "outside of the call center network" but are available from any public network and accessible with the call center employees' login credentials.
- Processes that introduce unnecessary risks that could lead to a privacy breach.
- Unnecessary exposure of personal identifiable information or confidential information to the call center employees.

- Unnecessary capabilities within call center applications that could lead to theft, privacy breaches or fraudulent activity.

Timeline:

1. Full Security Risk Assessment Phase: A full Security Risk Assessment will be conducted within an appropriate amount of time after program launch. Risks are identified and validated based upon a defined risk profile including other unique risks, and all the necessary reviews and approvals will be completed.
2. Share Risks and Remediation Strategies Phase: TP formally shares the risks and recommends remediation strategies with the applicable client. TP Leadership will also communicate risk summaries with client contacts during business reviews.
3. Implement Countermeasures Phase: Implementation of agreed upon risk remediation strategies and maintained compliance with those strategies going forward.
4. Repeat Process Phase: The Security Risk Assessment is repeated annually to identify potential new risks and improve the effectiveness of the overall process. Mid cycle risk assessment surveys are also communicated to business owners for response and documentation of any new tools, process or risks uncovered.

7. Global Privacy, Risk & Compliance Programs

The Global Privacy, Risk & Compliance Office is the Groups independent function responsible for maintaining, updating, and ensuring compliance with the TP Group Data Privacy Policy, Global AI Policy, and the Global Compliance Policy, which sets out the principles and requirements that TP must adhere to in order to comply with all applicable laws and regulations.

Key elements of the Privacy & Compliance Programs include:

- Binding Corporate Rules (BCR)
  TP received approval for both Controller and Processor BCRs from the French Data Protection Authority (CNIL). These are maintained and regularly updated by the Global Privacy & Compliance Office.
- ISO 27701 Privacy Information Management System
  TP companies in possession of an ISO 27001 certification are also ISO 27701 certified. The implementation of this global certification is the responsibility of the Global Privacy, Risk & Compliance Office.
- ISO 37001 Anti-Bribery Management System
  This is a global certification, extended to cover the entire Global Anti-Corruption Program.
- ISO 37301 Compliance Management System
  This is a global certification covering the Global Compliance Program which includes Third-Party Risk Management, Health & Safety, Trust & Safety, ESG and overall corporate compliance.
- Global HIPAA and Health Compliance
  The Senior Vice President of Global Privacy (SVP), along with the relevant stakeholders, maintain a Global HIPAA and Health Compliance Program to ensure even safer use and handling of protected health information when TP is acting as data processor on behalf of our clients.
- Global Data Retention
  TP's Global Data Retention Policy ensures that TP (1) retains records for such periods necessary to meet appropriate legal obligations and operational needs, and (2) routinely disposes of unnecessary records in the normal course of business under the approved Global Record Retention Schedule.
- Global Compliance Program
  Our Global Compliance Program establishes essential principles and policies to be adhered to by all TP employees in the conduct of TP's business, consistent with our company's values and applicable laws and regulations. This program also oversees the effective implementation of our Global Anti-Corruption Program.
- Global Third-Party Risk Management
  This program, overseen by the SVP of Global Compliance & Risk and Global CISO, ensures that risks arising from TP's involvement with Third-Party Risk Management (TPRM) third parties are identified and suitably addressed.
- Global AI Program
  The new Global AI Program is fully integrated into the Security, Privacy, and Compliance Programs, and manages the compliance with all applicable laws and obligations related to AI and establishes a set of AI Principles that ensure all AI Systems are managed in a trustworthy and ethical manner.

8. Third Party Risk Management

The TPRM Policy defines the governance framework and requirements for the TPRM Program to ensure effective oversight of TPRM third parties ensuring that TPRM third-party risks are identified and suitably addressed in a proportionate, risk-based manner.

The TPRM Committee, made up of the SVP of Global Compliance & Risk, Global CISO and other risk partners, shall support the development and approval of the TPRM Program and TPRM Policy through a vendor risk assessment. Each risk partner shall be responsible for identifying requirements under applicable laws and regulations, policies and contractual requirements within their respective areas of expertise.

In compliance with the Compliance Principles, the TPRM Program shall include the following elements:

- Purpose (including legal or regulatory requirements)
- Oversight & Governance
- Roles & Responsibilities
- Evaluation of identified risks and vulnerability management
- Third party risk monitoring
- Implementation Approach
- Independent audit assessment
- Training & Awareness

Definitions:

Compliance Principles – Every Privacy & Compliance Program must define the following minimum elements:

- Purpose (including legal or regulatory requirements)
- Oversight & Governance
- Roles & Responsibilities
- Key Risks (Definition & Reporting)
- Controls (commensurate to the risk: retired when no longer justified)
- Implementation Approach
- Training & Awareness

Risk Partners – Those functions within TP with significant responsibility for defining requirements under applicable law and regulation, ensuring compliance, or overseeing risk, including Corporate Legal, Global Ethics Hotline, Corporate Compliance team (including Anti-Corruption & Sanctions), Government Interactions, Ethical Business Practices and Sourcing (CSR), InfoSec & Cyber Security, Procurement, Privacy and Data Protection, Finance and Insurance Risk.

9. Global AI Program

The Global AI Program is a fully integrated program across Privacy, Security, and Compliance. The program focuses on ensuring all AI Systems designed, developed, deployed, and used in TP adheres to the set of AI Principles:

- Reliability – All AI Systems should consistently operate in accordance with their intended purpose and scope, and at the desired level of precision.
- Safety – All AI Systems should be designed and implemented with safeguards in place to protect against harm to people, business, and property.
- Accountability – Human oversight and responsibility should be embedded across the AI Lifecycle to manage risk and ensure compliance with applicable laws and obligations.

  The fundamental principle is that AI Systems should not be in control of human actions. Oversight, governance, and of course control should always be in the hands of a human being.

  The Executive Committee are accountable for all AI Systems implemented across the organization, and that they comply with the requirements set out in the Global AI Policy.
- Security – Robust and resilient practices shall be implemented to safeguard AI Systems through Security and Privacy-by-Design and Default.

- Privacy & Data Protection - AI Systems shall be designed to comply with applicable laws and obligations related to the privacy of personal data through the implementation of Privacy-by-Design and Default.

  Personal data used in training AI Systems should be collected in compliance with applicable laws and obligations, obtaining consent where required, retained for as long as the data is needed, deleted when it is no longer required. Personal data shall only be used for processing in line with what it was collected for. Where the processing goes beyond what it was originally collected for, additional consent shall be obtained.

  All personal data in any AI System shall have the ability to be deleted in line with the Global Data Retention Policy and the Data Retention Schedule.

- Transparency - Accurate disclosure shall be made available to all stakeholders to provide a clear understanding of what is happening in the AI Systems and what purpose they are designed for.

  All AI systems shall be designed to ensure that users are notified that they are interacting with an AI System, that an AI System is part of the process or that they are receiving output generated by AI Systems. This information must be included to ensure user disclosure and awareness.

- Explainability - All AI Systems shall be developed and delivered in a way that is capable of being explained in simple terms of how any conclusions were drawn from the AI System.

  All AI Systems developed shall have standardized information on the AI System, its function, and outputs, including information on the dataset used for the AI System training, validation, reinforcement and updating where applicable.

  The AI Addendum clarifies the ownership and usage rights of TP on client data, Client Inputs and Outputs. It also clarifies neither TP, or its suppliers shall use client data to train the AI Systems or solutions without the clients' prior authorization. The AI Addendum once signed, grants TP the right to anonymize client data and use anonymized data to improve its solutions.

  Where the organization is using Partner or supplier AI Systems, possible gaps or lack of information may be apparent in fulfilling obligations related to Explainability. Appropriate remediation plans shall be enacted with the relevant suppliers where necessary. Where these gaps exist to such an extent and the supplier is unwilling or unable to provide sufficient information for TP to comply with its legal, and ethical obligations to a level that TP will accept, the AI System may need to be reviewed for its use in certain jurisdictions and withdrawn/limited in its use.

- Fairness & Non-Discrimination – All AI Systems shall be designed to reduce bias to the minimum levels possible, or eliminate it from impacting individuals, or groups of individuals.

  All AI Systems shall ensure the ability for users to give feedback on the AI Systems function and output is available to them.

  All AI Systems shall be monitored throughout their entire life cycle for any changes in relation to its output in relation to bias or discrimination.

10. CISO Business Office

The CISO Business Office (CBO) serves as the strategic backbone of TP's global security operations, overseeing critical functions such as budget governance, vendor strategy, cybersecurity architecture and

assurance, global account security, and coordination with Holding Company CISOs (e.g., Specialized Services, Infinity).

Cybersecurity Architecture & Assurance

The Architecture team establishes a forward-looking security reference framework that embeds "Security by Design" and a "Security Comes First" mindset across the enterprise. The Assurance team conducts global technology assessments and gap analyses to strengthen key performance and risk indicators, ensuring resilience against evolving cyber threats.

Security Product Management & AI Security Governance

This team leads the lifecycle management of proprietary and custom-built security solutions, while spearheading the development and implementation of AI Security Governance across TP's global footprint.

InfoSec Account Management (iSAM) & SPDRI

These teams reinforce TP's global security infrastructure by applying deep expertise in technology, risk, and compliance. They drive standardized processes to uphold contractual and regulatory commitments with the highest level of security excellence across all regions.

Holding Companies CISO Office

Specialized Services and TP Infinity collaborate cross-functionally to align cybersecurity strategies with TP's business units, reducing internal risk and optimizing operational outcomes.

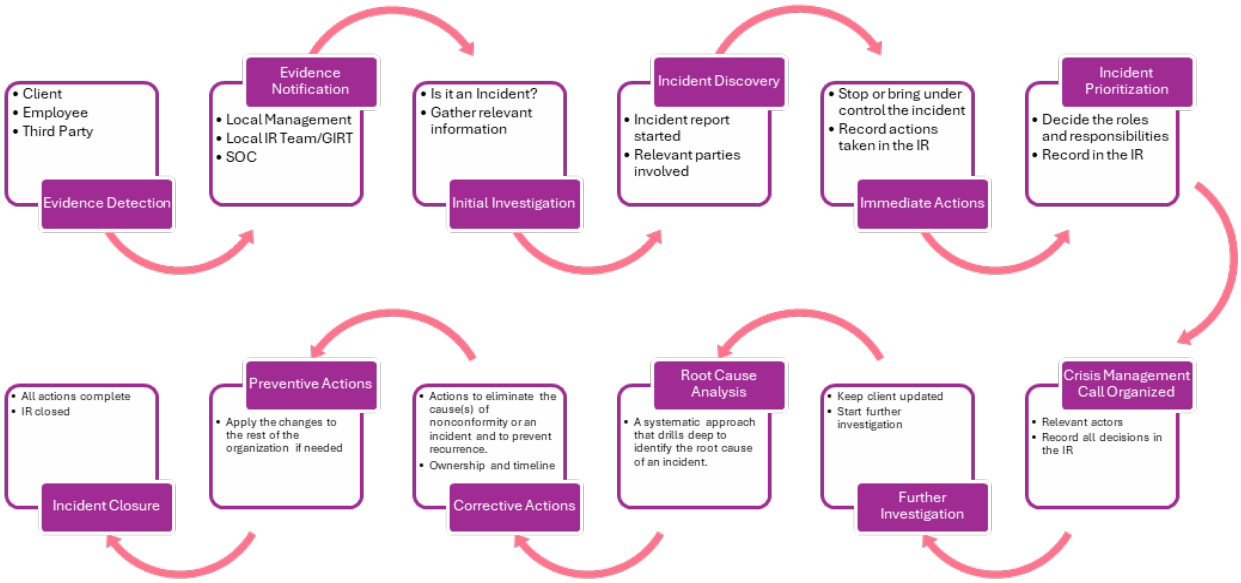
Security Program Office

Dedicated to strategic alignment and execution, this office ensures initiatives are delivered on time and within scope. It fosters global cohesion across security teams and facilitates seamless communication with stakeholders beyond the security function.

11. Global Incident Response Procedure

The Global Incident Response Procedure (GIRP) focuses on incident management, eradication, and risk reduction. In addition to ensuring all phases of the incident response process are completed (discovery, reporting, recovery, post-incident analysis), the Global Incident Response Team (GIRT) is the leadership team responsible for investigating and managing Events, Incidents and Weaknesses identified within any system or facility operated by TP or any of its Affiliates; and focuses, among other tasks, on remediating similar risks across similar programs. The incident response procedure safeguards TP from potential loss of revenue. Addressing wrong doings and protecting data throughout the incident response procedure include countless tasks and responsibilities for the GIRT, Security Operations Center (SOC), Regional Security Team, Executive Vice-President (EVP)/ client services lead/ Senior Account Manager (SAM), local incident response team, Privacy Office, and local or global Legal.

GIRT follows the NIST centralized/coordinated body model approach of handling incident response investigations for the organization and coordinates its efforts with regional and local incident response teams. In addition to managing the process, GIRT leads investigations into complex, critical, and top client-related incidents.



12. Global Security Operations Center (GSOC)

TP maintains a robust, globally integrated Security Operations Center (SOC) that provides continuous 24x7x365 monitoring and incident response across all IT environments, including both Selling, General & Administrative (SG&A) systems and client-facing production infrastructure. The Global SOC operates under a "follow-the-sun" model with physical and virtual presence in various countries around the globe, ensuring uninterrupted coverage and timely response.

Security analysts perform real-time monitoring using industry-leading Security Information and Event Management (SIEM) platforms, with a particular focus on end-user behavior analytics. The SOC also oversees global threat intelligence (external threat monitoring), penetration testing, red teaming, and security engineering support for the enterprise IT organization.

All Global SOC and Regional SOC roles, workflows, and controls are aligned with recognized industry standards and regulatory frameworks, including NIST SP 800-181 Rev. 1, NIST SP 800-53 Rev. 4, PCI DSS, and ISO/IEC 27001. This alignment ensures that TP security operations meet rigorous audit and compliance requirements, support effective risk management, and uphold the integrity of enterprise-wide cybersecurity governance.

13. Technical Security Controls

Anti-Malware System

All TP user end-points and servers are required to have the capability to prevent malware from impacting operations and from compromising the confidentiality, integrity, and availability of our IT platforms.

Endpoint Detection Response

All TP user end-points and servers are required to have the capability to detect and prevent information security incidents using anomaly, behavior-based technologies that are monitored and updated in real time with the latest known indicators of compromise and attack. Additionally, the end-point detection and response tools have the capability to isolate a suspected compromised host and allow for remote access to that host for incident response and forensic investigations.

Email Security Solutions

All email systems are protected, both inbound and outbound, against malicious attachments and internet links. Additionally, emails from known and suspected compromised domains are dynamically blocked by a third-party industry leading technology.

Multi-factor Authentication

A second factor of authentication (e.g., SMS code, push notification, One Time Passcode), in addition to username and password, is required for all TP employees to connect remotely to the Wide Area Network, Office 365 applications and all other TP provided email.

Remote Access Control

Remote access is managed using Virtual Private Network (VPN) tunnels or secure connections provided by Virtual Desktop Infrastructure solutions. Access is granted only after user and device authentication and successful device posture checks to ensure compliance with security policies.TP Protect

TP Protect provides additional security monitoring features that are proprietary to TP and are customized to meet the security needs of our clients and their service delivery. TP Protect can enhance monitoring, detection and prevention of fraud and payment card data breaches and can be tuned to the needs of our clients.

User Entity and Behavior Analytics (UEBA)

UEBA protects systems, environments, and users by identifying anomalies within an organization. These anomalies are then reviewed, and appropriate actions are taken to mitigate any risks. Essentially, UEBA is a security measure that helps TP detect and respond to unusual behavior that could indicate a security threat.

Webtraffic Security Control

All outbound internet traffic must pass through a secure next-generation proxy that enforces URL filtering, threat inspection, and data protection policies, with logs retained for monitoring and auditing.

14. Information Security Policies & Standards

Acceptable Use Policy

This policy defines the acceptable use of TP information and Information Assets.

Access Management Policy

This policy defines the requirements for secure access to TP Information Assets for which TP has operational control.

Asset Management Policy

This policy establishes the minimum requirements and responsibilities for the protection of TP information, equipment, and Storage Media assets throughout the asset lifecycle.

Communications Security Policy

This policy defines the requirements for establishing the network controls related to the TP network infrastructure and the Information Systems with that infrastructure.

Human Resources Security Policy

The intent of the TP Human Resources Security Policy is to establish the information security-related requirements throughout the Workforce Member lifecycle from recruiting and contracting through employment separation or termination.

Information Security Aspects of Business Continuity Management Policy

This policy defines the requirements for developing, testing, and maintaining the TP Business Continuity Plan for information security continuity. The requirements address the continuity of information security management and controls during a disruption of critical business operations.

Information Security Incident Management Policy

This policy defines the requirements for reporting and responding to security and Privacy Incidents involving TP information systems and operations.

Operational Compliance Policy

This policy defines the compliance requirements, processes, risk identification practices, audit and assessment and audit requirements.

Operations Security Policy

This policy defines the requirements for operations security to ensure dependable and secure day-to-day operations of Information Systems.

Organization of Information Security Policy

This policy establishes the information security roles and responsibilities required to implement and operate the TP information security program and applicable policies.

To be effective, information security must be a team effort involving the participation and support of every TP subsidiary, department, and Workforce Member who deals with information and Information Systems.

Specific information security roles and responsibilities must be formally assigned for the management and operations of the information security program.

Physical and Environmental Security Policy

This policy defines the requirements for establishing appropriate physical access controls to safeguard all TP facilities, Information Assets, and Workforce Members.

Risk Management Policy

This policy defines the requirements the establishment, operation, and maintenance the Risk Management Program as the basis for the larger Information Security Management System.

Social Media Policy

This policy establishes requirements for the appropriate use of personal and official TP Social Media platforms to protect Client data and ensure all posts referencing or related to TP are professional, consistent with TP values and messaging, and compliant with local laws.

Supplier Relationships Policy

The policy defines requirements for Third-Party management to maintain the same "in-house" level of data and privacy protection when using third parties.

System Acquisition, Development, and Maintenance Policy

This policy defines requirements for the identification of appropriate and applicable security controls for new Information Systems or enhancements to existing Information Systems.

15. Global Privacy & Compliance Standards

The Global Privacy & Compliance Office sets out the following set of Global Privacy & Compliance Standards (GPCS):

GPCS – 00 Introduction

This standard sets out the terminology and an overview of the standards.

GPCS – 01 – Privacy & Data Protection

This standard sets out the minimum requirements of the Global Privacy Program.

GPCS – 02 – Data Retention

This standard sets out the minimum requirements of how TP ensures data is retained across the organization.

GPCS – 03 – Health Insurance Portability Accountability Act

This standard sets out the specific requirements related to the Health Insurance Portability Accountability Act (HIPAA) for TP.

GPCS – 04 – Privacy by Design & Default

This standard sets out the requirements related to achieving Privacy-by-Design and Default. This includes the Technology, Privacy & Security Committee (TPSC), and Data Privacy Impact Assessments.

GPCS – 05 - Compliance

This standard sets out the minimum requirements of the Global Compliance Program.

GPCS – 06 – Third-Party Risk Management (TPRM)

This standard sets out the requirements for the Third-Party Risk Management Program.

GPCS – 07 – Compliance – Anti-Corruption

This standard sets out the minimum requirements for the Global Anti-Corruption Program.

GPCS – 08 – Compliance – Financial Conduct Authority (FCA)

This standard covers the specific requirements for TP UK in relation to its status as a Financial Conduct Authority regulated business.

GPCS – 09 – Compliance – Human Resources

This standard sets out the requirements of the Global Compliance Program related to Human Resources.

GPCS – 10 – Compliance – Finance

This standard sets out the requirements of the Global Compliance Program related to Finance.

GPCS – 11 – AI Use & Ethical Governance

This standard sets out the minimum requirements for designing, developing, deploying, and using AI Systems in TP.

16. Security Awareness and Culture

At TP, we believe that while robust technologies, policies, and processes are essential to defending against cyber threats, an informed and engaged workforce is the cornerstone of a resilient cybersecurity posture.TP is committed to fostering a culture of security awareness across all levels of the organization. Every new hire is required to complete and pass mandatory security training, which introduces key policies, reinforces the importance of protecting client data and promotes a secure workplace. To ensure continued awareness, all employees must complete annual refresher security courses that reflect the latest threat landscape and policy updates. To ensure relevance and impact, TP delivers role-based training tailored to specific job functions, enabling employees to understand and apply security principles directly within their areas of responsibility.

Beyond formal training, TP drives continuous engagement through a multi-channel awareness strategy. This includes physical and digital touchpoints such as strategically placed on-site posters, desktop wallpapers with security reminders, and targeted communications that reinforce key messages.

A highlight of TP's commitment to awareness is its annual Cybersecurity Awareness Month, which features interactive campaigns, team challenges, and educational content designed to deepen understanding and encourage proactive security behaviors. These initiatives are complemented by TP's confidential reporting hotline, which empowers employees to report potential issues or suspected misconduct, reinforcing a culture of accountability and vigilance.

17. Continuous Improvement

To ensure TP policies, standards and processes are current and aligned with evolving cybersecurity trends, a formal review is carried out annually or upon the occurrence of significant changes. These changes may include, but are not limited to, updates in regulatory compliance requirements, adoption of new technologies, emergence of novel threat vectors, or shifts in internal incident patterns. This proactive governance approach ensures TP maintains a resilient and forward-looking security posture across its global operations.

tp.com