Teleperformance
each interaction matters

Teleperformance Information Security and Privacy Program

An Overview

Table of Contents

Message from the Global Chief Information Security Officer

Teleperformance takes its clients' data security very seriously and has made major investments to ensure its readiness to identify, protect against, respond to, and recover from even the most sophisticated cyber threats. Our strategic objectives are to: 1- Prevent business disruption to client service delivery, 2- Prevent a data breach within our client and corporate environments, 3- Protect our business processes from compromise, and 4- Detect and prevent fraud. We achieve these objectives by employing industry leading information security technology, aligning to industry best practices (ISO 27,001, ISO 27,701, PCI DSS, HIPAA/HITRUST, NIST Cyber Security Framework), maintaining a highly trained information security staff and augmenting such industry leading technology with Teleperformance proprietary security products.

Teleperformance's number one security control is its cyber-aware staff and customer facing agents. We have an aggressive and comprehensive global security awareness training program which ensures our preparedness to resist even the most sophisticated threats.

We provide 24x7x365 security monitoring and response from our two global, follow the sun, Security Operations Centers in Greece, and the Philippines. Additionally, we have a global fraud and incident investigation team positioned in seven countries poised to support client investigations and incident management. This team operates in English, Spanish, and Portuguese, as well as local languages in India and the Philippines.

Our focus is to prevent rogue access to our environment by maintaining 100% multifactor remote access for all our employees. Additionally, we use the latest endpoint detection and response technology to prevent ransomware and other major cyber-attacks from having business impact. Our Global Security Operations Centers conduct continuous hunting activities for advance threats, and Teleperformance retains a third-party service that continuously hunts within our environment as a second pair of eyes.

The Teleperformance IT infrastructure is annually assessed consistent with ISO 27,001, ISO 27,701, PCI DSS and HIPAA/HITRUST (where required), providing third party attestation that we maintain the appropriate level of security controls expected by our clients. Many of our major service delivery centers can provide a SOC 2, Type II external audit of security controls as an additional proof point of our alignment to industry best practices and standards.

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

Very Respectfully,

Jeff Schilling
Global CISO

1. Introduction

For over 40 years, Teleperformance, the global leader in customer experience management, has been connecting customers with the world's most successful companies! Teleperformance employs over 380,000 people worldwide, operating from 83 countries, servicing over 170 countries and more than 265 dialects. To protect our clients' security, we constantly adapt to new technologies, monitor risks and threats, and comply with international regulations on data privacy. Teleperformance is committed to ensuring information security, compliance, and protecting the privacy and personal data of every individual, including its employees, suppliers, customers, business partners, clients and their respective end customers. This is achieved through industry leading policies, standards and control management as well as constant evolution of internal and external market trends and requirements.

2. Information Security Program Overview

Teleperformance 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 training, and monitoring security metrics to assess the achievement of our security objectives.

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

The Global Chief Information Security Officer leads Teleperformance'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.

Teleperformance Enhanced Cyber Security Program:

- 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

Security Principles

People: extensive cyber security training across TP

- Extensive cybersecurity training in 16 languages completed by 380 000 people
- Dedicated security organization
- C-level Security Governance

Process: security by design, 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

Teleperformance 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

ISO 27701:2019

ISO 27001:2013

The Payment Card Industry Data Security Standard

Recognitions

FROST & SULLIVAN
2019 BEST PRACTICES AWARD
GLOBAL BPO COMPLIANCE SECURITY & PRIVACY COMPETITIVE STRATEGY INNOVATION AND LEADERSHIP AWARD

Frost & Sullivan Competitive Strategy Innovation and Leadership Award for global best practices in compliance, security, privacy.

HPE-IAPP Privacy Innovation Award in the Privacy Operations category.

Alignments

IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
NIST
FRAMEWORK

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

The Council, composed of Teleperformance 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.

IT and Security Global Infrastructure Committee Charter (ITSECC Charter)

The IT and Security Infrastructure Committee (ITSECC) is the TP principal governance body that oversees the IT and Security investment strategy and capability roadmap for TP's Core Business units.

The ITSECC, composed of Teleperformance Global functional and Regional senior leadership in IT and Security, is responsible for ensuring the IT and Security Infrastructure capabilities are align to the global business strategy, achieving the best value for the company, and delivering a consistent client experience in the delivery of revenue-generating services and back-office support.

Its mission is to provide Teleperformance with best of breed global IT and Security solutions with high value return on investment to meet the business needs of the company and our clients.

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. 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 Teleperformance'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, and data flow.

Internal Audit

Teleperformance auditors' review over 200 security 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

Teleperformance 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

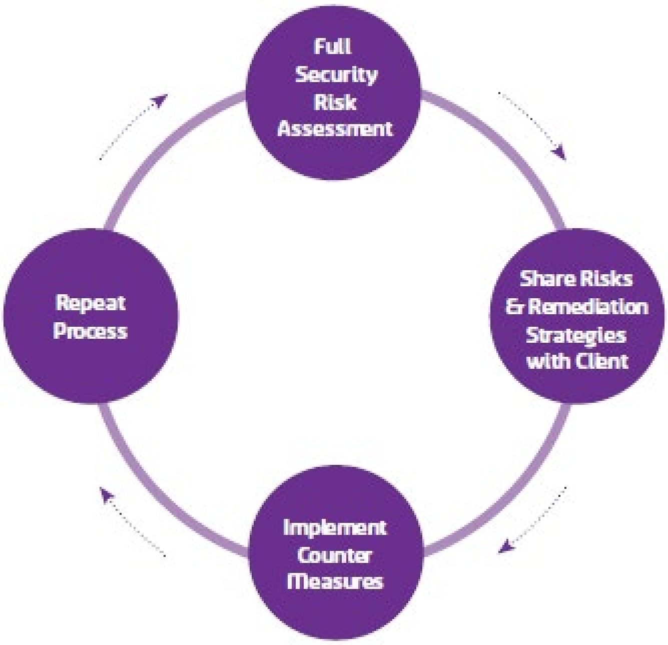
Our Security Risk Assessment is a proactive, non-intrusive method to identify potential risks in processes and applications within the call center environment. A Security Risk Assessment reduces risks for Teleperformance's clients and its customers while increasing privacy. The primary goal of a Security 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: Teleperformance formally shares the risks and recommended remediation strategies with the applicable client.
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.


Full Security Risk Assessment
Share Risks & Remediation Strategies with Client
Implement Counter Measures
Repeat Process

7. Data Privacy & Compliance Program

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

Key elements of the Privacy & Compliance Program include:

- **Binding Corporate Rules (BCR)**
  Teleperformance received BCR approval for both Controller and Processor from the French Data Protection Authority, CNIL. These are maintained and regularly updated by the Global Privacy & Compliance Office.
- **ISO 27701**
  The Teleperformance companies in possession of an ISO 27001 certification is also ISO 27701 certified. The implementation of this new global certification is the responsibility of the Global Privacy & Compliance Office.
- **Global HIPAA and Health Compliance**
  The Global Chief Privacy Officer (CPO) and Senior Vice President of Privacy (SVPP), along with the relevant stakeholders, are currently developing a stronger Global HIPAA and Health Compliance Program to enable even safer use and handling of protected health information when Teleperformance is acting as data processor on behalf of our clients.
- **Global Data Retention**
  Teleperformance's a Global Data Retention Policy ensures that Teleperformance (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 Conduct & Business Ethics**
  Our Global Conduct & Business Ethics Program establishes essential principles and policies to be adhered to by all Teleperformance employees in the conduct of Teleperformance'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 Global CPO and Global CISO, ensures that risks arising from Teleperformance's involvement with Third-Party Risk Management (TPRM) third parties are identified and suitably addressed.

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 Global CPO, Global CISO and other risk partners, shall support the development and approval of the TPRM Program and TPRM Policy through a vendor due diligence questionnaire and risk assessment process. Each risk partner shall be responsible for defining the key risks, definitions and reporting in 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
- Qualification Requirements (for Program Leads)
- Key Risks (Definition & Reporting)
- Controls (commensurate to the risk: retired when no longer justified)
- Implementation Approach
- Training & Awareness

Definitions

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

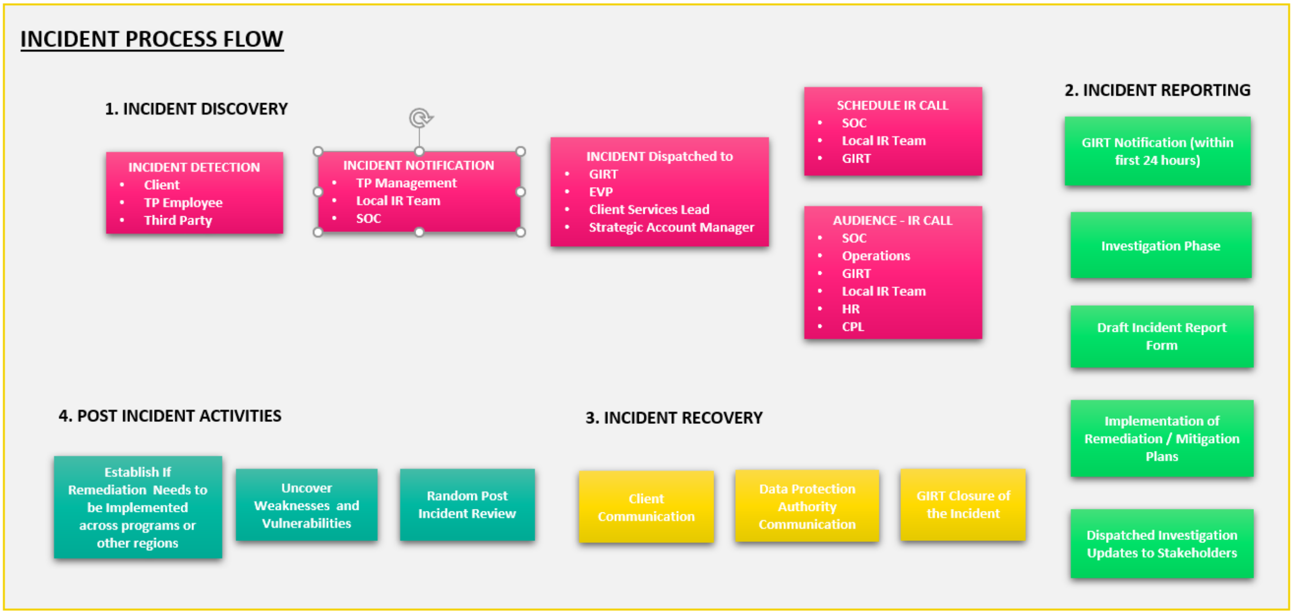
- Purpose (including legal or regulatory requirements)
- Oversight & Governance
- Roles & Responsibilities
- Qualification Requirements (for Program Leads)
- Key Risks (Definition & Reporting)
- Controls (commensurate to the risk: retired when no longer justified)
- Implementation Approach
- Training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

Risk Partners – Those functions within Teleperformance with significant responsibility for defining requirements under applicable law and regulation, ensuring compliance, or overseeing risk, including the Teleperformance Legal Department, 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.

9. Global Incident Response Process

The Global Incident Response Process (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) focuses on remediating similar risks across similar programs. The incident response process safeguards Teleperformance from potential loss of revenue. Addressing wrong doings and protecting data throughout the incident response process 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.

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



INCIDENT PROCESS FLOW

1. INCIDENT DISCOVERY

INCIDENT DETECTION
- Client
- TP Employee
- Third Party

INCIDENT NOTIFICATION
- TP Management
- Local IR Team
- SOC

INCIDENT Dispatched to
- GIRT
- EVP
- Client Services Lead
- Strategic Account Manager

SCHEDULE IR CALL
- SOC
- Local IR Team
- GIRT

AUDIENCE - IR CALL
- SOC
- Operations
- GIRT
- Local IR Team
- HR
- CPL

2. INCIDENT REPORTING

GIRT Notification (within first 24 hours)

Investigation Phase

Draft Incident Report Form

Implementation of Remediation / Mitigation Plans

Dispatched Investigation Updates to Stakeholders

3. INCIDENT RECOVERY

Client Communication

Data Protection Authority Communication

GIRT Closure of the Incident

4. POST INCIDENT ACTIVITIES

Establish If Remediation Needs to be Implemented across programs or other regions

Uncover Weaknesses and Vulnerabilities

Random Post Incident Review

10. Global Security Operations Center

Teleperformance provides 24x7x365 security monitoring and response for the global IT infrastructure including our Selling, General & Administrative (SG&A) back office and client facing production environments. The Global Security Operations Center (GSOC) uses a “follow the sun” model with physical/virtual environments in the Philippines and Greece. The GSOC provides the defense analysts role “eyes on glass” monitoring our global security logging with the best of breed Security Incident and Event Management (SIEM) tools, with an emphasis on end user behavior analysis. The GSOC manages Teleperformance’s global threat intelligence monitoring (outside in) and provides penetration testing and red teaming services. Additionally, the GSOC provides security engineering services to our global IT team. Each of the four Teleperformance regions have a Regional Security Operations Center (RSOC) that provides Computer Security Incident Response Teams (CSIRT) that perform forensic investigations and coordinate with regional and country level IT teams to resolve security incidents that require IT helpdesk first responder activities. All GSOC and RSOC positions and processes are aligned to industry best practice standards of NIST 800-181 rev 1, NIST 800-53 rev 4, PCI DSS and ISO 27,001.

11. Technical Security Controls

Anti-malware system

All Teleperformance 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.

End User and Detection Response

All Teleperformance 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 Teleperformance employees to connect remotely to the Wide Area Network, Office 365 applications and all other Teleperformance provided email.

Remote Access

Remote access is managed using Virtual Private Network tunnels or using secure connections provided by virtual desktop infrastructure solutions.

TP Protect

TP Protect provides additional security monitoring features that are proprietary to Teleperformance 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.

12. *Information Security Policies & Standards*

Acceptable Use Policy

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

Access Management Policy

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

Asset Management Policy

This policy establishes the minimum requirements and responsibilities for the protection of Teleperformance 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 Teleperformance network infrastructure and the Information Systems with that infrastructure.

Human Resources Security Policy

The intent of the Teleperformance 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 Teleperformance 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 Teleperformance 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 Teleperformance information security program and applicable policies.

To be effective, information security must be a team effort involving the participation and support of every Teleperformance 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 Teleperformance 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 Teleperformance Social Media platforms to protect Client data and ensure all posts referencing or related to Teleperformance are professional, consistent with Teleperformance 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.

13. Security Awareness and Training

Teleperformance has policies, standards, processes, and technologies in place to combat cyber threats and attacks. But Teleperformance believes that educated employees are one of the most important factors in an effective cyber security defense.

Teleperformance is invested in bringing security awareness to all its workforce. New hires are required to complete and pass the security training to create awareness of all policies, protect client data and maintain a safe and secure workplace. All employees are expected to take refresher security training courses annually. Aside from mandatory trainings, awareness is fostered through other communication channels. These include both physical and digital channels such as, but not limited to, posters placed strategically on-site and security reminders as desktop computer wallpapers. These different communication channels are leveraged to raise security awareness and encourage use of Teleperformance’s reporting hotline program that encourage reporting of potential issues or suspected wrongdoing.

14. Review and Development Process

To ensure Teleperformance policies, standards and processes are up-to-date or aligned with current security trends, a review is carried out annually or whenever a significant change occurs. Such changes may include, but are not limited to, compliance with regulatory standards, use of new technologies, new/emerging threats, or company incident trends.

For more information:
teleperformance.com

Follow us:

- teleperformanceblog.com
- /company/teleperformance
- /teleperformanceglobal
- @teleperformance
- @teleperformance_group
- /teleperformance

Teleperformance
each interaction matters