Willis Towers Watson

Information Cyber Security and Data Privacy Overview

Version 3.1

The information provided in this document is for Willis Towers Watson and its subsidiaries. This property is confidential to Willis Towers Watson and is solely for the use of clients and prospective clients in evaluating Willis Towers Watson's capability as a provider of services.

Willis Towers Watson

willistowerswatson.com

Introduction

Willis Towers Watson recognizes that effective management of information security and risk is an essential part of maintaining the trust and confidence of our clients. We take a proactive approach to information protection and security, and our information security and data protection strategy is designed around the principle of defense in depth. We place tremendous importance on maintaining the confidentiality of data provided to us by our clients and colleagues and continue to make significant investments in our information security and data privacy program.

This overview is directed to clients and prospective clients of Willis Towers Watson and its subsidiaries and provides a summary of the safeguards and processes we have in place and are essential to maintaining our reputation as a trusted advisor.

Scope

The scope of our information security program includes all parts of Willis Towers Watson globally, including subsidiaries, colleagues, contractors, and third-party suppliers that may process information on our behalf or have incidental access to data.

Code of Conduct (Code)

Our commitment to protecting the confidentiality of client information is a key component of our Code and requires all colleagues to respect the confidentiality of information about our clients' businesses, employees, and customers. Our Code requires all colleagues to adhere to the laws specific to the countries and regions where they support our clients, to respect the confidentiality of information about our clients' businesses, employees, and customers, and to comply with the information security and data privacy policies, along with the regulatory requirements applicable to their work. The Code must be read and acknowledged by all colleagues when they join Willis Towers Watson and annually on completion of the Data Privacy and Protection and Information Security training module.

Security Function

Security is everyone's responsibility and everyone at Willis Towers Watson has a role in ensuring the security of the information that is entrusted with us. In addition to our colleagues, our dedicated security team is comprised of individuals with proven expertise and defined roles and responsibilities who lead specific functions within our global information security program.

The Chief Information Security Officer (CISO) leads the function and is responsible for determining the strategy for the organization and for implementing our global information security program. Our Information Security and Privacy Committee provides additional oversight of our security and privacy policies and programs, and our Board has responsibility for Willis Towers Watson's overall security posture.

The committee works to review and approve our Information Security and Data Privacy Policies annually. These policies form the basis for relevant control standards for the organization.

Information Security Management System (ISMS)

Willis Towers Watson has a well-defined risk-based Information Security Management System, aligned to ISO/IEC 27001:2013. It is designed to protect information according to the following security principles:

Confidentiality: Protect information assets against unauthorized disclosure and unauthorized access.

Integrity: Protect information assets from unauthorized changes, to safeguard the accuracy and completeness of information and processing methods.

Availability: Ensure information assets are only used by authorized individuals or processes when required.

The objective of our Information Security Management System and associated policies, guidelines and procedures are to enable our colleagues to provide a consistently high level of service both internally and to our clients, while ensuring an appropriate level of security. Willis Towers Watson's global information security program is assessed as part of its external and internal ISO/IEC 27001:2013audit and associated maintenance of certification. We are subjected to multiple audits throughout the course of the year that demonstrate the maturity of our information security posture.

Data Privacy Program

Our data privacy principles reflect the data privacy and data protection laws applicable to our operations. Our approach includes:

Notice and Authorization:	Explaining to each client the types of personal data we need for our work and obtaining the proper authorization to use that data in connection with our work.
Relevance:	Limiting the personal data, we collect to the minimum needed for our work and using it only as authorized.
Transparency and Use:	Providing notice as appropriate regarding what information is collected and the purposes for which it will be used.
Security:	Maintaining appropriate security measures to safeguard personal data from accidental loss or unauthorized access, alteration, use or disclosure.
Access:	Limiting access to information to authorized individuals and entities.
Safe Transfer:	Requiring any affiliate or subcontractor to whom we transfer personal data to protect it in an appropriate manner and obtaining proper authorization to transfer personal data if required.
Regulatory Compliance:	The Global Privacy Office works on an ongoing basis with our compliance teams to ensure awareness of legal developments and any upcoming requirements and compliance with those applicable to Willis Towers Watson.

Roles and Responsibilities

Everyone at Willis Towers Watson has an active role to play in ensuring the security of information in accordance with its policies and any other associated guidance that may be issued from time to time.

Information Security at Willis Towers Watson is built on the principles of defense in depth and the intent to Know-Protect-Report:

Know – the information security requirements and behaviors expected of Willis Towers Watson colleagues by understanding its Information Security Policy and taking the mandatory training.

Protect – Willis Towers Watson information and that of our clients, colleagues by following those requirements and displaying those behaviors.

Report – any information security incidents or suspicious activity by following the established Willis Towers Watson cyber-security incident response process.

Appendix

This Appendix provides additional detail about the information security and data privacy programs maintained by Willis Towers Watson. It addresses certain controls put in place for items of interest to our clients' security and privacy representatives.

Outsourced Support Functions

Willis Towers Watson relies on different outsourced IT providers to manage and support selected portions of our IT environment. Willis Towers Watson requires that these suppliers and service providers follow our security standards and policies, and industry best practices. Our Security Function completes a security review process for each supplier providing outsourced IT services to Willis Towers Watson based on risk.

Willis Towers Watson maintains oversight over these outsourced IT relationships. Our oversight program is designed to make sure these suppliers operate in accordance with all contractual commitments made to Willis Towers Watson from an operational, security and business perspective. Examples of the oversight measures employed may include, but are not limited to, reviews of external audit reports, certifications relevant to the services, onsite reviews of supplier's facilities and processes, periodic operational metric and scorecard reviews, internal audits, and involvement in the change and problem management processes.

Cyber Security Defence – Incident Response

Cyber Security Defence Incident Response service is a combination of the Global Security Operations Centre (GSOC), Global Major Incident Response Team (GMIRT), Global Information Cyber Security Incident Handling Team (GIIHT), Cyber Threat Intelligence Team (CTI) and Cyber Platforms Security Team (CPST) where Analysts and Specialists Triage, Investigate and Respond to Security incidents. Built on a Security Incident Event Management (SIEM) platform that provides advanced activity analytics to identify, prevent, and respond to attacks and infiltrations that is monitored 24X7 by the GSOC team with expertise in technical investigations and the GMIRT expertise in conducting Digital Forensics.

Willis Towers Watson (WTW) has a global Information Cyber Security Incident Response Plan (ICSIRP) for identifying and managing cyber and data security threats, including those with the potential to adversely affect information security and data privacy, globally. The ICSIRP defines the roles and responsibilities of WTW stakeholders involved with responding to cyber and data security events, severity levels, and threat categories, and outlines a process for incident management, including escalation and communication procedures. The ICSIRP is reviewed and tested annually.

The ICSIRP requires that each incident be logged, stakeholders notified, incidents investigated, and necessary actions taken. Incidents are managed daily, with input from WTW stakeholders including all Cyber Security Defence Incident Response service teams, and in collaboration with our Global Privacy Office's Legal and Compliance teams (Office of the General Counsel/Privacy), to address immediate concerns and identify patterns, trends, and areas of potential improvement. Actions taken pursuant to the foregoing process depend upon any number of underlying circumstances, including the nature and severity of an incident. The following is an illustration of the typical process for a security incident involving an unauthorized data disclosure:

- **Reporting**: WTW colleagues are required to report data security events that they become aware of, including an unauthorized data disclosure, via dedicated reporting portals that direct the reports to the GSOC team for assessment.

- **Triaging**: GSOC's assessment of reported data security events include triage and categorizing according to nature and severity. GSOC engages relevant WTW stakeholders and other Cyber Security Defence teams, e.g.,GMIRT, CTI,and Privacy, as appropriate.

- **Legal review**: Incidents warranting Office of the General Counsel/Privacy's engagement include those involving unauthorized data disclosures. Privacy for the geography in which the incident involves affected data subjects is engaged by GSOC and sent details of the incident, including any applicable documents, e.g., Contracts. Privacy reviews information about the incident and advises on, and assist with, any required actions, including any legal obligations for data breaches, e.g., mitigation, remediation, regulatory reporting, law enforcement reporting, notification to data subject and/or data owner, contractual notifications to clients, etc. Privacy also communicates with regulators about reportable incidents as may be required by governing local laws.

- **Mitigation**: GSOC coordinates efforts with WTW stakeholders and resolver groups, e.g., business unit leads, Privacy to consider ways to mitigate the effects of an incident, including as may involve an unauthorized data disclosure, e.g., if data were transmitted to a known unauthorized recipient, then WTW seeks confirmation that the data will not be misused, e.g., recipient has deleted the data, not disseminated the data, not retained any copies of the data.

- **Longer term remediation**: Once priority actions have been taken, longer term remediation steps are considered depending upon the root cause of the incident, e.g., reviews of and improvements to the process, additional training for those responsible for causing the event, etc.

Records Management Program

Willis Towers Watson has responsibilities for records retention throughout the world and has an established Global Records Management Program to oversee the establishment of appropriate policies and standards.

The program's principles are to:

- Keep all business records, which may affect substantially the obligations of the company, no longer than necessary to meet legal, regulatory, and business obligations in compliance with the company Records Retention schedule; this reasonably assures the availability of those records when needed.
- Provide for the disposition of records in the normal course of business when their retention has expired, except in cases where such records are subject to an active Legal Hold.

- Identify and safeguard vital records and incorporate such procedures into any disaster recovery plan.
- Provide adequate protection and security for all records, including those subjects to data privacy requirements.

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets.

We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance.

Together, we unlock potential.

Learn more at willistowerswatson.com.