PRIVACY SECURED - UNISYS INFORMATION SECURITY AND DATA POLICIES AND PROCEDURES OVERVIEW

PROTECTING PERSONAL DATA WITH OPERATIONAL SECURITY

UNISYS | Securing Your Tomorrow®

Information and information systems are vital to our increasingly digital and connected world. As a global Information Technology (IT) company that specializes in providing solutions with leading-edge security to clients in government and commercial markets, Unisys understands the need to respect privacy and protect personal data without impeding the demands of today's worldwide information exchange.

Dedicated to protecting critical data from threats such as theft, fraud, misuse and disaster, Unisys employs rigorous measures to protect personal information while in use and at rest, the media where it is stored, the systems that process it, and the methods by which it is transmitted. This protection works to ensure the integrity, availability and confidentiality of information and information systems.

Data Processor Privacy Protection

Organizations that collect personal information are mandated to protect and ensure it is used in a way that respects the privacy of the individual whose personal details they collected. These organizations must thoroughly vet and select entities that will process this personal information to assure that the proper security and privacy measures are in place both within the processor's organization and any sub-processors entrusted with the organization's data.

External threats and regulatory requirements are constantly evolving, demanding an IT partner that handles valuable client information with care, possesses a firm understanding of operational needs and maintains a proactive approach to anticipating and addressing future requirements in the evolving security landscape.

Proven Expertise and Technology

For more than a century, Unisys has built a reputation for deep, reliable technical expertise to help businesses and governments protect their information assets and apply processes and technology to achieve new levels of competitiveness and success. Trusted by leading organizations around the world, Unisys delivers integrated solutions to clients with critical infrastructure upon which society depends on daily.

At the heart of every solution we design and every system we deploy is an understanding that our clients need their information, including personal data, to be protected and properly used. Our team of experienced privacy and information security technologists develop and enforce strategies that continually meet the needs of our clients around the globe. Our commitment to upholding the highest standards of privacy is proven through our privacy and security practices.

Corporate Governance

Corporate governance is the cornerstone of the privacy practice at Unisys, and we are dedicated to getting it right. Unisys maintains a strong corporate governance structure for privacy, ethics and information security, and is committed to protecting the personal data of our clients, associates, vendors, and partners.

The Compliance and Ethics Office is a function within the law department at Unisys responsible for establishing, maintaining, and implementing appropriate policies and processes to protect the privacy of personal data collected or processed in compliance with privacy laws, regulations, and standards applicable to our business. Led by the Chief Compliance and Privacy Officer, the office focus is on embedding privacy by design throught the organization. The central privacy office is supported by a network of lawyers, data protection officers and both functional and business unit privacy leads. All personnel are members of the International Association of Privacy Professionals (IAPP). The team includes Certified Information Privacy Professionals for the EU, Asia, US and a Certified Information Privacy Manager.

Unisys is a corporate member of the IAPP and supports the membership of key personnel in the company in various functions, including solution design, legal, compliance and contracting. We participate in continued education through IAPP and other privacy organizations around the world.

The Corporate Security and Infrastructure Office (CSIO) provides guidance and direction for information security activities for all organizational units at Unisys. The CSIO is responsible for establishing and maintaining corporate information security policies, developing and implementing information security measures, and embedding security into the network and infrastructure.

As a multinational company with operations around the world, Unisys complies with applicable laws and regulations. This includes policies and regulations about personal information protection, such as sector-specific and breach notification laws in the U.S., EU, Brazil data protection laws, and other country-specific privacy laws around the world. Maintaining the integrity and confidentiality of personal data that we collect, process, and store is how we build and maintain the trust that is critical to the way we conduct our business activities.

UNISYS PRIVACY PRINCIPLES

We process personal data for the purpose(s) for which it was provided to us.

We use technical and organizational security measures to limit accessing and processing of personal data to Unisys associates, contractors, vendors, and others who require access for the performance of their obligations to Unisys and in accordance with the purpose for which the data was collected.

We only disclose personal data to third parties (including our contractors, vendors, partners, customers and others) who agree to comply with applicable data protection and privacy laws and agree to implement and maintain appropriate technical and organizational security measures to safeguard the personal data. We will also disclose personal data when required by law or for a valid business purpose, for example, due diligence to comply with regulatory obligations or when necessary for a transfer of business operations pursuant to a merger or acquisition.

We comply with applicable laws when transferring personal data within Unisys or to third parties by utilizing a combination of data transfer agreements, consent, and Standard Contractual Clauses, in addition to maintaining appropriate technical and organizational security measures to protect the personal data.

Personnel Qualifications

Unisys conducts a pre-employment screening to the extent permissible and in accordance with applicable local labor laws and statutory regulations. Once hired, we require all personnel to complete a confidentiality agreement as a condition of employment and follow policies on the protection of personal data, confidential information and information security procedures.

Information security and compliance is the responsibility of every Unisys associate. Associates receive annual mandatory training and updates online training in ethics, privacy and information security awareness when hired and throughout their employment at Unisys, Content is updated annually to maintain relevancy. Training topics include the protection of personal data, back-ups, security of offsite equipment, access control, endpoint security, data transfers, country and function-specific privacy issues, confidentiality, integrity, and continuity. Comprehension is tested during the interactive modules and completion is tracked and documented online. Further education and training on privacy and security risks is provided based on client requirements, evolving technology and regulation, and targeted associates roles and responsibilities. Additional awareness campaigns run throughout the year.

Unisys maintains a Code of Business Conduct and Ethics and policies related to privacy and information security. The Compliance and Ethics Office has a reporting, investigation and disciplinary process to address concerns and violations of security or privacy policies. Discipline, up to and including termination, is behnchmarked across the organization and determined based on the circumstances, severity and local law.

Vendor Management

Unisys conducts due diligence on the privacy and security practices of third parties entrusted to provide services and process personal information for us and our clients. Unisys requires third-party vendors storing or handling client data to agree to certain contractual and legal requirements regarding personal data protection, including requirements for prompt notification and handling of data incidents. Unisys manages subcontractors' performance and exercises the right to audit them as needed.

Accountability

Unisys security actively monitors systems, environments, and data to identify threats to our environment. Unisys policies and standards define log retention schedules.

Unisys complies with all mandatory audits and participates in other regulatory inspections. Additionally, our internal audit function continuously evaluates and improves our internal risk management, control, and governance.

Questions or concerns regarding privacy can be filed at www.unisyscompliance.com. All queries are logged and tracked in this compliance application, which is accessible internally and externally. Ethics, compliance, or company policy questions can be asked anonymously and status monitored at this site.

For non-HR data, we encourage parties to resolve concerns with us directly. EU/Swiss individuals may bring an issue through the JAMS alternative dispute resolution process at www.jamsadr.com/eu-us-privacy-shield.

The Chief Compliance Office, Internal Audit, and Security Operations work together to infuse best practices into the organization, ensure compliance, and resolve incidents. Unisys privacy practices are reviewed and audited regularly.

Data Flow

Unisys has global privacy practices for processing personal data in compliance with applicable data protection laws. We transfer personal data between the countries in which we operate in accordance with the standards and conditions of these laws, including standards and conditions related to security and processing. When processing personal data on behalf of our clients, we will provide a list of any third parties who may receive client personal data. Unisys will refrain from the transfer of personal data to third parties if a written exception is provided by the data controller. All personal data transmitted over public networks is encrypted.

As a global IT services company and employer, Unisys processes personal data governed by the EU General Data Protection Regulation (GDPR) and country specific data protection laws from its service centers outside of the European Economic Area (EEA) countries, including centers in the U.S., India, Philippines, Brazil, Colombia, and China. Unisys transfers personal data from EEA countries to the U.S. and non-EEA-located centers under data transfer mechanisms permitted by the GDPR.

To meet these GDPR requirements Unisys non-European legal entities processing personal data of EEA residents have executed intragroup data processing agreements with Unisys EEA entities that provide services to our clients. Unisys Corporation relies on Standard Contractual Clauses approved and published by the EU Commission for all transfers of personal data from the EEA to non-EEA Unisys entities.

If, in performing services for its clients, Unisys transfers personal data to a third party (such as a subcontractor), Unisys enters into a data processing agreement with the third party that requires such third party to adhere to similar data processing terms as a sub-processor to Unisys.

Information Security

As a company that provides security solutions to our clients, security is part of our DNA. We take a holistic approach to the information that we protect, for both our employees and our clients. Our baseline security standard is NIST 800-53, but we follow all regulatory guidance regarding management and disclosure throughout all countries in which we operate. Rather than separating out physical and cyber security, we look at the overall risk to information, and take proactive steps to minimize that risk. We look at each and all ingress and egress points for our information—whether in the cloud, sitting in a data center, or on a laptop—and make sure that we're doing everything that we can to keep that information secure. Through automation with our tools and procedures, we track every piece of data moving through our systems and analyze it for the type of data, who's touching or transmitting it, and why. If those tools find something suspicious, they'll generate alerts that go through our security orchestration and response teams to further assess potential threats.

Operational Security

Unisys' managed digital service centers and data centers are certified to ISO standards, including ISO 9001, ISO 20000, ISO 27001 and ISO 22301. We conduct annual internal security assessments and facilitate external independent verification and validation audits to maintain these certifications. SSAE SOC 1 Type II audits of all major digital service centers and data centers are performed each year and copies of the most recent certifications and assessment reports are available to data controllers upon request.

For our client engagements, Unisys uses multi-tiered application architecture for a robust Internet presence. This architecture applies levels of network security commensurate with business needs and the value of the information resources protected.

Physical Security

Unisys adheres to strict security controls to prevent unauthorized parties from accessing the locations containing personal data.

A dedicated Security Officer is responsible for implementing access procedures and controls to areas within Unisys locations that contain personal data.

Unisys locations are secured with badge-controlled access at the entry points and additional controls such as multi-factor authentication are implemented for access into sensitive areas. Requests for access must be approved by the employee's manager as well as the responsible owner for the secured area. All physical entry controls and access rights are regularly reviewed and updated.

Logical Security

Application access is provided on a least privileges basis and requires a unique user account name, ID and password.

Hardened workstations and end-point security solutions provide additional layers of system security and only approved software and browsers with the necessary security features are available. Unisys uses hard disk encryption software to protect user systems.

Incident Management

Unisys follows a Privacy Incident Response Plan when there is a suspected or actual breach of personal data. Privacy incidents are detected using our Security Incident Response Process that details the handling of information security events affecting the integrity, confidentiality, authentication, non-repudiation and availability of information as well as IT infrastructure.

To monitor for incidents, Unisys utilizes an enterprise-wide network intrusion detection system and extensive firewall protection infrastructure. Network sensors and firewalls are located at key points throughout the worldwide network.

Events and status updates from the devices are fed to centralized management systems and forwarded to a consolidated monitoring and reporting system for Security Information and Event Management (SIEM).

The Unisys SIEM is deployed across the Unisys intranet and uses pattern-based analysis technology to process highly complex decision logic in real time. It continuously learns environmental behavior by cross-correlating log information and delivers both real-time alerting and historical forensics. The fully virtualized architecture scales easily to provide secure, partitioned views.

All incidents are resolved in a time-bound manner. Root causes and key learnings are examined, documented and reviewed for ongoing quality and improvement purposes. Unisys maintains a well-defined incident management framework which ensures that security events are given utmost priority. The framework can receive both manual and automated notifications on a variety of incidents and prioritize them until resolved and root-cause analysis completed.

If an incident involves client data, Unisys provides prompt notification to the client and cooperation to enable the client to follow its incident response process. This includes close coordination between Unisys and the client's incident response teams and sharing of resources in order to contain, assess, mitigate and prevent incidents. Unisys also maintains Professional Liability insurance coverage for monetary damages Unisys is legally obligated to pay resulting from a data breach due to Unisys failure.

PRIVACY INCIDENT RESPONSE PLAN

Unisys follows a Privacy Incident Response Plan when there is a suspected or actual breach of personal data. Four key principles drive this response:

- Breach containment and assessment
- Evaluation of the risks associated with the breach
- Notification
- Prevention of future breaches

Disaster Recovery

Unisys maintains Disaster Recovery (DR) and Business Continuity Plans (BCP) for our data centers, managed service centers, and delivery locations that are regularly revised and updated to meet our expanding activities and services. Our current plans are designed to minimize the potential impact of a disruptive event to the services we provide our clients.

Unisys aligns the Business Continuity Management System (BCMS) framework to ISO 22301:2012. BCMS policy outlines the focus on personnel safety and the need to maintain base line BCPs. Additionally, all BCPs are reviewed and tested annually and whenever there is any significant change made to the plan.t. In addition, Unisys develops a specific business continuity plan for services provided to clients during transition as agreed to by the client.

Each data center where personal data is stored is backed up to a geographically diverse data center or the cloud. Physical protection against damages from natural and manmade disaster is implemented at these locations and they are adequately protected from power failures with multiple feeds, uninterruptible power supplies, backup generators and other supporting utilities. Equipment is maintained in accordance with recommended service intervals and applications are routinely backed up according to schedule. In addition, regular restore tests are performed and encryption is enabled for tape backup.

Retention and Destruction

Unisys mandates media handling and secure destruction standards for the safe and permanent destruction of personal data that is no longer required. Unisys conforms to Department of Defense standards for the secure disposal of electronic media containing confidential information. All data on Unisys issued End-User Technology is Microsoft Bitlocker™ encrypted. Unisys also ensures the secure destruction of paper documents, including the provision of burn bins at all Unisys locations.

Unisys maintains a document retention program. We follow document retention guidelines based on the type, location and classification of the data retained.

Trusted Privacy Partner

Protecting client information is a top priority at Unisys. We have the deep expertise, dedicated resources and proven technology for robust protection of personal information. We work with our clients to identify and design privacy and security practices that meet their operational needs.

LOCAL LAWS, OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES, AND LEGAL REQUESTS FOR CLIENT INFORMATION

Unisys has implemented measures to regulate the disclosure of client data to a government entity. These measures require us to consider our obligations to comply with any order or demand and any legal obligations to protect our customer's Personal Data or Confidential Information. With regard to data of EU residents, Unisys abides by the obligations set forth in any legal mechanism relied on for data transfers to third countries, such as Section III of the Annex to the European Commission Implementing Decision on Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679.

Specifically, to the extent permitted by law, we will promptly notify the customer of the order or demand before we respond. If we are not permitted to provide notification to the customer, we will seek permission to notify the customer or ask the issuing court or government authority to seek the requested documents directly from the customer.

We will challenge an order or demand when appropriate and valid legal grounds exist. If production is required to comply with a valid Order or Demand, we will disclose the minimum amount of customer Personal Data or Confidential Information necessary to comply.

For more detailed information about information privacy and security policies and procedures at Unisys go to www.unisys.com/unisys-legal/privacy or contact unisysglobalprivacy@unisys.com

For more information visit www.unisys.com

07/21

21-0344