Washington University in St. Louis

Information Security Customer Statement

The Washington University - School of Medicine has a long history of providing reliable and trustworthy information. It maintains this reputation through a variety of means, not least of which is a comprehensive IT and information security management framework supported by a wide range of security policies and guidelines.

This document explains the universities approach to information security and describes the methods and mechanisms used to protect its information and information systems. It is designed to answer questions our customers regularly ask to satisfy their own legal and regulatory requirements. If you have additional questions, please do not hesitate to contact the Washington University - School of Medicine Information Security Officer.

Oversight and strategy

The University's information security is directed by the Information Security Office (ISO) with support from a core group of security liaisons. This extended team of managers and staff is devoted to ensuring that the University receives advice and support on how to apply existing and evolving security practices and mechanisms to protect the University's proprietary information and maintain compliance to the various regulatory bodies. This group is comprised with senior business and IT officers who ensure that information security risks are identified and managed to the University's standard. Strategy, oversight and governance of information security are provided through the Office of the CIO.

The University's strategy seeks to strike a balance between the need for strong security controls on the one hand, and ease of use and cost effectiveness on the other. This is achieved through the application of demonstrable security controls at an appropriate level to the service being offered. Furthermore, our security strategy ensures appropriate security controls exist within service design and operation. This is to counter the threats to confidentiality, integrity and availability of customer or University protected information, which is stored, transmitted, processed or otherwise handled within our systems and communications networks.

Washington University in St. Louis ensures it has staff trained to identify issues and resolve them as quickly as possible with minimal impact on its customers.

Policies and standards

The University's Information Security and Risk Practice actively develop and maintain information security policies. These are closely aligned with international standard – ISO 27001 Code of Practice for Information Security Management. ISO 27001 was originally developed to provide a set of controls comprising best practices in information security, and has evolved as the de-facto reference for identifying the controls needed to assure confidentiality, integrity and availability of business and health information systems. Policies and standards are regularly reviewed to take account of evolving technical risks as well as regulatory changes and customers' needs for information security.

Network and host security

Our products and services are offered through public and private networks. There are a wide range of tiered controls to ensure the appropriate level of protection to systems and data in transit. Vulnerability scanning of our internet-facing sites is undertaken regularly and policy compliance software is used to ensure systems are maintained in accordance with security requirements. Penetration testing companies are engaged to provide a further level of assurance.

Malware/malicious code

In accordance with industry practices, Washington University - School of Medicine utilizes many techniques to protect its IT systems from malicious software and other attacks. Prime examples include:

- **Alerting** – Security alerts for new threats are received from a variety of sources including software vendors and CERT organizations. These alerts are evaluated by security specialists and circulated across the company with instructions on mitigating actions.

- **Protection** – Protection measures include the application of patches, hotfixes, and other configuration workarounds that have been recommended by software vendors. Other methods of protection include the use of anti-virus software, filters and intrusion detection. Firewall filters to block out bound communication to known malware command and control servers.

- **Controls** – The service delivery of many Washington University - School of Medicine products relies on Personal Computers (PCs) as the main interface to customers. Where specialized software is supplied to allow the PC to run as a 'Washington University - School of Medicine Desktop', rigorous controls are applied at all stages of development, testing and software distribution of the code to prevent viruses, 'trojan horses' or other malicious code.

Business continuity

As part of the focus on customer service and product resilience, Washington University - School of Medicine maintains a Business Continuity and Disaster Recovery Program. The program is designed to prepare our staff to achieve an effective state of readiness to handle a broad range of events that may threaten the safety of our employees, the continuity of our services and the protection of business operations and assets. We achieve this by:

- Technological and operation resilience
- The protection of Washington University - School of Medicine staff and assets
- Enabling recovery of critical processes and systems in the event of a major disruption or disaster
- Meeting regulatory requirements defining business continuity as 'the planning that allows us to ensure the safety and welfare of its employees and the continuance of its critical business functions to either prevent or minimize the impact of any disruption of its services to its customers. It also identifies the requirements for alternative workspaces and access to systems, data and infrastructure to maintain critical processes and the incident management framework to manage the recovery of the business in the event of a disruption'. The aim is to maximize the technological resiliency of the networks and systems infrastructure and provide back-up in the event that the service resilience measures fail.

Such measures may include fault tolerant systems, automated failover, load sharing or balancing and network server redundancy.

More information on Washington University - School of Medicine Business Continuity Program can be obtained from your Washington University - School of Medicine Information Security Officer

Physical security

All major Datacenters meet Washington University - School of Medicine Corporate Technical Policy guidelines. The University's guidelines include requirements for physical security, building maintenance, fire suppression, air conditioning, UPS with generator back-up, and access to diversely delivered power and communications. Periodic audits and reviews are conducted that determines the recovery level of the site.

A variety of methods are used to control access to Washington University - School of Medicine sites and depending on the sensitivity of the facility, may include some or all of the following: the use of security staff, ID cards, electronic access control systems incorporating proximity card readers, pin numbers or biometric devices.

Monitoring and audit

Automated and systematic checking of systems, services and operations are undertaken to ensure compliance with policy, and effectiveness of applied security controls. Network management, Intrusion Detection, SIEM and other security tools are also implemented and operationally managed to monitor and maintain a highly secure systems environment.

The Internal Audit department functions independently from all Operations and Development activities. The department gives advice and assurance on the controls within Washington University - School of Medicine production systems. Its staff includes both professionally qualified auditors and staff with specific technology backgrounds.

Privacy/data protection compliance program

Policy/compliance program

The Washington University - School of Medicine respects privacy and seeks to protect personal data in accordance with its privacy policy. The universities privacy and security policies cover areas such as access control, authentication, audit, monitoring, data storage and back-up, and transmission standards.

Further inquires may be directed to:

Kevin Hardcastle, CISSP
Chief Information Security Officer
Washington University in St. Louis
hardcastlek@wustl.edu
314.747.2305
https:/informationsecurity.wustl.edu