

# WileyPLUS Information Security Practices

(Updated Summer 2007)



*Since May 2005, over one-half million students have purchased access to WileyPLUS for use in one of more than 3,000 classes. Wiley recognizes how important the data WileyPLUS collects is to faculty and students. To that end, Wiley's data security practices are robust, meeting and often exceeding industry standards. We continually review our policies against industry guidelines such as [FERPA](#) and support those standards. A more detailed explanation about how Wiley sustains this level of security for WileyPLUS follows.*

**Founded in 1807,** John Wiley & Sons, Inc. has grown and evolved, taking pride in its ability to meet the changing needs of its customers. Throughout its two hundred year history, Wiley has maintained a continuous commitment to quality and serving the needs of its customers. Consistent with this commitment, the software, content and hosting architectures of *WileyPLUS* offer a high degree of reliability, redundancy, and security at multiple levels. The results of these efforts speak for themselves. *WileyPLUS* customers receive the highest levels of performance dependability in the industry. Our system availability continues to average over 99% since its launch, well above the norm for this kind of application.

#### **Secure Facilities:**

In keeping with Wiley's overall security practices, *WileyPLUS* is hosted in a secure **Level 8 Data Center** with 24x7 access restrictions and controls. Both physical authorization controls and rules are used and monitored.

#### **Secure and Redundant Architectures and Business Continuity Measures:**

Wiley takes a best practices approach to managing its Internet hosting environment and infrastructure. These practices include state-of-the-art, redundant databases, disk storage systems and storage area networks, further protected with daily incremental and weekly full backups of all applications including the entire *WileyPLUS* suite of resources. Backup tapes are rotated offsite daily with a company specializing in secure offsite storage. Wiley maintains a comprehensive disaster recovery plan and regularly conducts recovery tests.

Key security measures and provisions include:

#### **Secure networks:**

- Centralized monitoring of up-to-date, worldwide firewalls
- Proactive network and risk management
- Multi-level virus detection and spam protection
- Intrusion detection systems
- Proactive, global CERT CC Advisory communications and management

#### **Practices that insure ongoing security:**

- Regular, objective, third party security scans and audits of Demilitarized zones (DMZ's)
- Internal and external access controls
- Appropriate division of labor as additional system safeguards and data protection layers.
- Restricting employee access to data to a "need to know" basis
- Maintaining compliance with Wiley's corporate [privacy policy](#), and requiring adherence by all employees who have access to student and instructor data.

Of course, no security system is foolproof. But we feel confident that the *WileyPLUS* team is continuously working to ensure the highest level of quality, professionalism and reliability our customers have come to associate with the Wiley name.