Unum UK
Our Information Security

Our products

Income Protection, Life Insurance, Critical Illness Insurance, Dental and Optical Cover providing financial protection for today's workforce.

Our commitment

We are committed to earning and keeping your trust and confidence. Our integrated approach to security and data protection is embedded throughout our business and ensures we remain highly diligent, compliant with industry and regulatory requirements, and adaptive to changing threats.

Protecting your information

We demonstrate our continued commitment to keeping the data we hold safe and secure through successfully achieving SOC2 Type 2 and Cyber Essentials Plus Compliance. Unum does not complete Information Security Questionnaires but these assurance documents can be provided on request.

Our two main offices in Dorking and Basingstoke have audited and controlled external and internal access - with manned reception areas during office hours and security patrols overnight. Access and activities within data centres and other secure areas are strictly controlled.

Strategy

Our information security strategy is designed to mitigate business risks of:

- Improper disclosure/loss of information assets
- Service disruption
- Data corruption

This also continues to satisfy increasing regulatory requirements for robust security controls.

Our strategy specifically tackles cybersecurity risk, insider and data handling risks, and availability of service.

Policies and Risk Management

We operate a comprehensive Information Security policy which is documented on our Intranet. All employees are made aware of the IT Acceptable Use Policy at the beginning of their employment or contract.

All staff undertake mandatory annual Privacy and Information Security training supplemented with regular phishing testing, additional training and communications to promote awareness.

To ensure we meet, or surpass, our embedded industry standards and Privacy Regulatory requirements, the Information Security team continually analyse risks and drive an all-inclusive programme of mitigation activities and control improvements. To maintain and improve our security programme, we implement and monitor a comprehensive suite of controls spanning governance, policies, standards, procedures, and multiple layers of technical defences.

Governance

Our UK security programme is overseen by the Unum UK Senior Manager, IT Information Security & Risk, reporting into both the Group SVP Chief Information Security Officer (CISO) and the UK Chief Information and Digital Officer (UK CIDO).

A regular Information Security Committee meets to ensure appropriate governance, coordination, and business involvement. Additional review, challenge and support are provided by the UK Executive Committee and the Board.

Information and Data Protection

We employ a Data Protection Officer who has overall responsibility for Data Protection. All business data provided to Unum by customers is treated as confidential. Our email system ensures that TLS is used wherever possible, and has additional capability to encrypt confidential or secret data. Data Loss Prevention and monitoring tools are used, while memory sticks and USB drives are not permitted for data storage. We encrypt all laptops and backups. We also operate a clear desk policy and have implemented secure release printing.

Technical and network security

Our defence-in-depth strategy has multiple layers of security throughout our computing environment.

- The Unum network perimeter is protected by layers of firewalls, DMZs, and Intrusion Prevention Systems (IPS) with definitions updated regularly. These systems run 24/7 to monitor our systems for cyber threats and provide alerts.
- Industry leading security tools filter malicious email and web traffic, and block unauthorised access to servers and workstations.
- Configuration standards for servers and systems are defined in formal procedures, with default system accounts disabled.
- Anti-malware and other security hygiene tools are deployed at multiple layers.
- Patching processes and tools ensure the environment is updated in a proactive and timely manner.
- Secure remote working is enabled through company-issued laptops and secure VPN with multi-factor authentication.
- Industry-leading network access controls prevent any unauthorised devices from connecting to our network.
- Third party security tools routinely scan the internal network and external perimeter to detect vulnerabilities and identify any malicious activity.
- Independent penetration testing and specialist security assessments ensure our infrastructure and applications are resilient to external threats.
- Our Software Development Life Cycle is supported by an established project methodology, robust change, release & incident management processes and Static/ Dynamic code scanning.

Threat intelligence is monitored and acted upon by our Security Operations Center (SOC), supported by the expertise of industry-leading managed security monitoring services.

Cyber threats

Cyber resilience is a critical objective. Recognising that cyber-crime is not unique to Unum or our industry, we engage with our security vendors, other businesses and specialist organisations (such as FS-ISAC) to share information about cyber threats. We routinely engage independent security specialists to test and assess our capabilities - strengthening both our security, and our ability to stay current and respond effectively to emerging threats.

Access management

All assets and user access is authorised through a centralised process. New starters, role changes and terminations are managed through processes linking our HR system with the IT service desk. Access is allocated based on job requirements and removed upon termination. The access policy requires strong password standards including:

- Minimum password lengths
- Complexity
- Enforced password changes
- No password re-use
- Account locking following consecutive incorrect passwords

Administrative access is tightly controlled and monitored. Privileged accounts are highly secured using a privileged Account Management and password vaulting solution. All access is reviewed every 6 months and all user accounts with 30 days of inactivity are flagged for investigation.

Business resiliency

We use industry-standard backup and recovery software. Data is backed up daily with encryption. We perform an annual disaster recovery exercise as well as Global Incident Management Team exercises, which include cyber incident scenarios.

Our comprehensive business continuity framework covers loss of facilities (buildings), loss of people and loss of IT. Our incident management process follows ITIL best practices, including the handling of security breaches according to clearly defined protocols and using external specialists if needed. We constantly review procedures to ensure we continue to meet industry best practice, assuring our customers of our strength and commitment to both protecting their information and maintaining our high quality of service.

Regulatory information

Unum is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. We are registered with the Information Commissioners Office and we have full insurance arrangements in place which reflect our responsibilities as a Data Controller and ensure we maintain a mutual Data Controller relationship with our customers.

unum.co.uk