LEXIPOL SECURITY & PRIVACY CONTROLS

Lexipol takes the security of our enterprise and Software-as-a-Service (SaaS) products (KMS policy management solution, Cordico wellness solution and Academy learning management systems) very seriously.

We hold ourselves to compliance with the **NIST 800-53 R5** Security and Privacy Controls for Information Systems and Organizations. This standard was produced by a joint task force for the National Institute of Standards and Technology in the U.S. Department of Commerce. Following is an overview of the significant elements of our security and privacy controls.

TESTING & ANALYSIS

- Annual security audit against **NIST 800-53 R5**, conducted by an outside firm.
- Annual pen testing of all SaaS products, performed by an outside, independent firm that employs "white hat hacker" cybersecurity tactics.
- Continuous vulnerability testing by an independent firm.
- Continuous network and system vulnerability testing using software that Lexipol licenses.
- Static analysis of our software, looking for vulnerabilities every time it is built.

ACCESS CONTROLS

- Lexipol's SaaS products utilize a proprietary **Oauth2 Identity Access Management** (IAM) system that supports **SAML2** for integration with customer AD implementation (which inherits the customer's authentication security requirements). While Lexipol SaaS products run in a variety of environments (private cloud, Azure and AWS), the IAM runs in the **AWS GovCloud.** Passwords are stored using PBKDF2 with 180,000 iterations that utilize SHA256 Hash.
- All interactions with Lexipol SaaS products pass through **Web Access Firewalls,** using https, encrypted using **TLS 1.1+**. At rest, all data storage and backups are encrypted with **AES256** and conform to **FIPS 140-2**.
- User and Admin access (all data transmission) is through browser-based encrypted interfaces. Lexipol's mobile apps use the same browser-based interfaces, using **https**.
- Lexipol complies with **CCPA** as well as **GDPR** for user data privacy.
- Lexipol uses partners that comply with **PCI** and does not keep credit card information on hand.
- Lexipol never utilizes or stores Social Security numbers or personal health information.

SECURITY POLICIES

Lexipol maintains and annually reviews internal policies pertaining to the following topics:

- Acceptable Use Policy
- Audit & Accountability Policy
- Certification & Accreditation Policy
- Configuration Management Policy
- Contingency Planning Policy
- Data Breach Policy
- Data Encryption Policy
- Company Data Protection Policy
- Lexipol Disaster Recovery Plan
- Identification & Authentication Policy
- Incident & Data Breach Response Plan
- Incident Response Policy
- Maintenance Policy
- Media Protection Policy
- Network & Server Standards
- Password Policy
- Personnel Security Policy
- Physical & Environmental Protection Policy
- Right to Erasure Policy
- Risk Assessment Policy
- Security Awareness & Training Policy
- Security Planning Policy
- System & Communications Protection Policy
- System & Information Integrity
- System & Services Acquisition Policy