Hugo Security and Privacy

Security and Compliance by Design - Our Approach to Security

Security Program and Organization

At Hugo we believe that it is our responsibility to deliver our services via secure networks, systems, and applications. We know confidentiality and security are extremely important for our customers. By using Hugo's services, customers leverage our robust security controls while still maintaining ownership of their data.

Hugo's Security Program utilizes industry-leading, risk-based, frameworks and standards. Hugo has a Security & Compliance team led by the Chief Trust Officer (CTO) who is responsible for the strategic development, implementation and monitoring of the security program within the company.

Hugo's Security Program utilizes industry-leading, risk-based, frameworks and standards. Hugo has a Security & Compliance team led by the Chief Trust Officer (CTO) who is responsible for the strategic development, implementation and monitoring of the security program within the company. Hugo's CTO also serves as the official Data Protection Officer (DPO). The CTO has previously held privacy and security leadership roles at Canonical, CIBC, Deloitte Consulting, European Commission, and the United Nations, among others. He holds a Master of Laws (LLM) in Internet Law & Policy specializing in Privacy, Security, and Cybercrime, and has obtained several industry certifications in corporate governance, cybersecurity, IT auditing, privacy, and business continuity.

This section will provide a high-level overview of how we secure our services, systems, networks, and applications.

Security Policies, Processes, and Procedures

Hugo has developed relevant policies, standards and procedures which are updated and approved annually by the Security & Compliance team and respective Executive owners. These policies are made available to all Hugo employees through our collaboration platform.

Information Security policies, standards, and procedures include:

- Information Security Policy;
- IT Acceptable Use Policy;
- IT Risk Management Policy;
- Access Control Policy;
- Security Incident Response Policy;
- Security Incident Response Procedures;
- Secure Software Development Life Cycle (SSDLC) Policy;
- Disaster Recovery and Business Continuity Policy;
- Information Classification and Protection Policy;
- Information Security in Supplier Relationships Policy;
- Storage Media Destruction Policy;
- Patch Management Policy;
- Physical and Environment Security Policy;
- Backup and Restore Policy;
- Change Management Policy;
- Software Asset Management Policy;
- Enterprise Asset Management Policy;
- Human Resources Security Policy;
- Acceptable Use of Generative AI Policy; and
- Product Cybersecurity Requirements Standard.

Risk Assessment, Control Activities and Risk Mitigation

The purpose of the Hugo risk assessment process is to identify, assess and manage risks that affect the organization's ability to achieve its objectives. Exposures defined by Hugo, consider both internal and external influences that may harm the entity's ability to provide reliable services. The risk assessment is updated bi-annually.

Infrastructure

Hugo is a cloud-first organization, and its operations are delivered using several third-party Software as a Service (SaaS) platforms. These include Google Workspace (collaboration), JumpCloud (device and identity management), Slack (messaging), FactorialHR (people operations), and Quickbooks (finance). Trellix is used for endpoint detection and response (EDR).

For end users, the organization uses standardized hardware that must be enrolled in JumpCloud for device management.

Data Communications

Traffic between the customer and Hugo is encrypted through a managed Virtual Private Network (VPN) hosted on AWS. The VPN utilizes the Blowfish cipher which has a 64-bit block size and a key length of 128 bits. It also uses 160-bit HMAC-SHA1 as a cryptographic signature on packets to protect from tampering.

Incident Resolution & User Support

Hugo has an established incident resolution and user support framework which employs Zendesk with Slack integration for ticketing and incident resolution. JumpCloud is employed for remote user support.

Disaster Recovery and Business Continuity

Hugo leverages a combination of distributed cloud availability zones as well as daily backups in AWS servers to ensure customer data is easily recoverable in the event of a disaster. Backup and disaster recovery plans are in place and regularly tested.

Security Awareness Training

Hugo leverages an integrated platform for security awareness training combined with simulated phishing attacks, e-learning, tips & tricks, Dark Web email exposure checks, and other advanced features. All Hugo personnel must complete security awareness training upon joining the organization. There are also annual training requirements for both privacy and security. Additionally, quarterly phishing campaigns are delivered to ensure that Hugo personnel remain vigilant with regards to online threats.

Compliance and Certifications

The organization's information security program is based on the NIST Cyber Security Framework (CSF) v2, Center for Internet Security (CSC) Critical Controls v8.1, and IEC/ISO 27001:2022. **Hugo is currently ISO 27001 and HITRUST certified**, which attests to our compliance with information security management system (ISMS) best practices. Our security controls are constantly evolving to keep up with the dynamic landscape of evolving threat actors.

Hugo is in the process of completing SOC 2 Type II and Cyber Verify independent audits.

Privacy by Design - Our Approach to Privacy

Compliance with Data Protection Laws and Regulations

Hugo is committed to compliance with data protection laws, regulations, and industry best practices. We have processes in place to stay up to date on the evolving global privacy landscape and to reflect changes within our operations. We demonstrate our accountability and dedication by building security and privacy into the DNA of our business and services at the start.

Hugo remains closely apprised of the requirements of the European Union's General Data Protection Regulation (GDPR) and the Nigeria Data Protection Regulation (NDPR). For EU and UK citizens, our collection and use of personal data is regulated by the UK GDPR which applies in the UK (alongside the UK Data Protection Act 2018) and the EU GDPR which applies across the EEA (together, the "GDPR"). We are responsible as a "controller" of that personal data for the purposes of those laws and as a "processor" when we are acting on behalf of our customers or other third parties.

Hugo demonstrates accountability for our handling of personal data by staying up to date with the evolution and introduction of privacy and data protection regulations across the world to quickly respond and maintain compliance.

As previously mentioned, we have appointed a competent individual to oversee design, implement, and monitor our privacy and data protection practices.

Protection of Customer Personal Data

As previously mentioned, we have appointed a competent individual to oversee design, implement, and monitor our privacy and data protection practices.

- Compliant with all relevant laws and regulations;
- Consistent with our needs and objectives;
- Created with enterprise-wide involvement; and
- Understood and supported enterprise-wide.

Policies and Procedures

Hugo has policies, procedures and standards to ensure that customer personal data is handled responsibly and in compliance with data protection principles, laws, and regulations. They are updated and approved annually by respective stakeholders and are made available for all Hugo employees via our centralized online document repository.

On an ongoing basis, we deliver privacy awareness training across our staff population and, where permitted, record completion. We review and record where and how our products and services collect, use, retain, and dispose of personal data. Risks are identified, recorded, and mitigated. Key policies, procedures, and standards are as follows:

- Customer Privacy Policy;
- Staff Privacy Policy;
- Data Breach Management Policy and Procedures;
- Data Retention and Disposal Policy;
- Data Protection Agreement (DPA) - Controller/ Processor and Dual Controller Relationships;
- Data Protection Impact Assessment;
- Standard Contractual Clauses (SCCs); and
- Register of Data Processing Activities (ROPA).

Lawfulness, Fairness, and Transparency

Hugo is transparent about how we collect, process, retain, and delete personal data. The personal data we collect, use, process and share depends on the particular services that have been requested and/or activities being carried out. For more information, please see our Customer Privacy Policy.

If Hugo becomes aware that any government authority (including law enforcement) wishes to obtain access to or a copy of some or all of our customers' personal data, whether on a voluntary or a mandatory basis, then unless legally prohibited or under a mandatory legal compulsion that requires otherwise then Hugo shall use commercially reasonable and lawful efforts to inform customers of such requests. Hugo will respond to the relevant authority that the request for access to Service Data should be notified to or served upon customers in writing, and where reasonable and lawful, challenge such prohibition or where reasonable.

In no event shall Hugo knowingly disclose personal data in a massive, disproportionate, and indiscriminate manner that goes beyond what is necessary in a democratic society. Hugo has not built any backdoors or other methods into its services to allow government authorities to circumvent its security measures and have access to personal data.

Purpose Limitation and Data Minimization

Hugo uses the personal data we collect in accordance with the relevant data protection rules and regulations. We are clear about the reasons we collect and use personal information and in a manner that is consistent with those purposes. We have data protection practices in place to ensure that any required use of personal data outside of the originally stated purpose is fair, lawful, and transparent.

Hugo's policies and procedures support data minimization. This includes limiting the collection and use of data to only that is necessary, granular data access, and a strict-need-to-know principle.

Data Retention and Storage Limitation

Hugo retains personal data we process on behalf of our customers, collected directly from our customers or about staff for as long as needed to provide the service to our customers or fulfill any contractual requirements. We may further retain and use this personal data as necessary, including but not limited to:

- Complying with our legal obligations (including in defense or pursuit of a legal claim);
- Maintaining accurate accounting;
- Financial and other operational records;
- Resolving disputes; and
- Enforcing our agreements.

Use of Data Processors

Hugo uses data processors to assist in providing our services to our customers. A data processor is a third-party service provider, who collects, processes, and retains personal data on behalf of Hugo, acting as the data controller. Prior to engaging with a data processor, Hugo uses our Vendor Security Assessment (VSA) toolkit to conduct a comprehensive security and privacy review of the data processor to ensure that their security and privacy program is adequate to our standards. Hugo understands that we are responsible for the personal data under our custody and control, even while it is being collected and processed by a data processor.

Hugo executes agreements with data processors before personal data is shared to ensure they fully understand their obligations, responsibilities, and liabilities.

Cross-border Transfers

Hugo does not currently operate in the EU. When receiving transfers from the EU, Hugo ensures that data is held in countries that the European Commission has determined to offer an adequate level of protection. In instances where countries fall outside of this list, we rely on Standard Contractual Clauses (SCCs) as a basis for transfer. This further includes conducting thorough assessments to ensure that technical measures and organizational measures such as policies and procedures support the level of adequacy.

When receiving data from the EEA, to ensure the protection of customers' personal data, Hugo also implements several additional technical, contractual, and organizational measures.

For more information, please see Section 1 on Security and Compliance by Design.

Notifications of Disclosures

In instances where access to personal data is requested by public authorities, Hugo will work to notify our customers of such requests if we are permitted to do so by law. Where possible, Hugo will provide the full details of the request.

If compelled to disclose any personal data to requesting authorities, Hugo shall only disclose the data to the extent that it is legally required in accordance with applicable law(s).

Compliance Program Updates

We are committed to maintaining the highest standards of privacy and data protection. We continuously monitor and assess our data protection practices identifying necessary improvements to ensure our practices are in line with market expectations and current practices.

Delivering the Future of Customer Experience, Today.

23/06/2024

OUTSOURCING+
hugo

NORTH AMERICA | EUROPE | AFRICA