fact sheet

Consilio Security Infrastructure Snapshot

Consilio has a robust enterprise security framework that includes all aspects of information security management, including business continuity, disaster recovery, vendor management, incident management, vulnerability management with third-party PEN testing, and an information privacy program with a DPO.

Infosec Team

We have a dedicated, global information security team with a broad range of industry experience and professional infosec certifications including ISO 27001 LA, CBCP, CBRA, CDPP, CEH, CISA, CISM, CISSP, CPISI, GAWN GCIA, GCIH, GCPN, GPEN, GPYC, GSE, GSEC, GWAPT, GXPN, OSCP, OWASP, and Security+.

Data Centers

- *Chicago*
- *Dallas*
- *Dusseldorf*
- *Frankfurt*
- *Hong Kong*
- *Ireland*
- *London*
- *Paris*
- *Shanghai*
- *Tokyo*
- *Toronto*
- *Virginia*
- *Zurich*

Certifications & Compliance

- ISO/IEC 27001:2013 certified
- ISO/IEC 27701:2019 certified
- HITRUST certified (CSF V9.3)
- ITAR compliant
- SOC2 Type 1 compliant (with audit report)
- Cyber Essentials Plus certified
- GDPR compliant
- CCPA compliant
- Compliant with EU-US and Swiss-US Privacy Shield principles*

Security Highlights

- Data centers are ISO 27001 certified or have completed SSAE 16/Type II audits and are protected by 24/7 security, alarms, motion detection, biometrics, man-trap entry doors, and locked cages
- Environmental controls to protect data centers from fire, water, natural disasters
- Near real-time data replication between disaster recovery facilities in each geographic region
- Strict least-privilege access controls to data centers, networks, and systems
- All data separated logically by client and project
- Data at rest: AES-XTS 256-bit encryption
- Data in transit: TLS 1.2 and 1.3 only, 128-bit/256-bit ciphers for symmetric encryption algorithms
- Multi-layer, multi-vendor, overlapping security model with redundant coverage against MITRE ATT&CK framework
- Pre-employment background checks and nondisclosure agreements
- Annual employee security training, continuous phishing awareness tests
- Secure virtual document review infrastructure with enhanced remote user security, MFA

***Although the EU struck down Privacy Shield, the US Department of Commerce still requires US entities to follow its principles. Refer to the FAQs at privacyshield.gov.**

Consilio Information Security Summary

Consilio offers eDiscovery, document review, risk management, and legal consulting services. We support multinational law firms and corporations using with legal and regulatory industry expertise and specialized tools. Consilio's Complete Security suite includes a team of licensed security experts following certified best practices.

Regulations: Consilio is certified for the ISO\IEC 27001:2013 and ISO/IEC 27701:2019 standards and HITRUST CSF V9.3, and meets all of their stringent requirements to appropriately handle sensitive data. All of Consilio's colocated data centers are either certified for ISO 27001 or have completed SOC 2 Type 2 audits. Consilio complies with ITAR regulations, EU-US and Swiss-US Privacy Shield principles (still applicable in the US), the EU General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and many other data privacy regulations across the globe. Consilio's data center and office locations in the UK are also certified for the Cyber Essentials Plus scheme.

Infosec Program & Policies: As required by our ISO 27001 and 27701 certifications, Consilio maintains overarching privacy and security policies and procedures that standardize our privacy and security posture across all our global locations. Enterprise privacy and information security policies and procedures are properly reviewed by management and provided to Consilio personnel. Policies and procedures are approved by the Consilio Privacy and Information Security Governance Council (PISGC), are communicated to all staff, and are reviewed annually. Our policies ensure that all data in Consilio's possession is handled in accordance with local data protection regulations, based upon legal and contractual requirements that vary at our different locations across the world. Compliance with these requirements is regularly monitored and audited by internal and external parties, including ISO auditors.

Our certifications require our policies to cover all privacy and security areas relevant to protecting data in our possession, including risk management, incident management, vendor management, disaster recovery/business continuity, network security, access control, human resources security, asset management, change management, and others.

Infosec Structure: Consilio's chief information security officer heads our highly qualified information security team, which manages all of the organization's privacy and information security activities. Within the information security team are separate teams dedicated to security operations, privacy, compliance, risk, identity, and access management. We also engage third-party, managed security providers for some advanced security functions, and we have personnel based in the EU to offer supplemental expertise for EU-related legal and privacy and compliance concerns. Privacy and information security initiatives are also overseen and supported by the Consilio PISGC, which consists of executives from various Consilio business units. The PISGC meets biannually to review and audit Consilio's privacy and information security posture.

Vendor Risk Management: Risk management is part of Consilio's holistic approach to privacy and security. As part of Consilio's vendor management program, all of our vendors must be vetted to ensure they do not pose unnecessary privacy or security risks to Consilio or our clients. Audits of Consilio's disaster recovery and business continuity programs are performed on a regularly scheduled basis. Internal audits are performed by Consilio's global information security team. Data backups are refreshed continuously and stored in our secondary data centers, located in facilities that are physically distanced from primary data centers.

Network Security: Consilio's computing networks are set up with a DMZ and multiple firewalls to separate internet-accessible network segments from sensitive data storage segments. Our networks are protected by stringent firewalls, third-party monitoring services, intrusion detection and prevention software, antivirus software, and strict access control policies. The user permissions process follows the principle of least privilege, and access to each network segment must be formally approved by appropriate authorities. Changes to IT infrastructure follow a formal change management process. Software is patched regularly and in a timely manner, subject to formal review and approval before being implemented.

Data Storage: All client data is physically and logically segregated from Consilio corporate data, and client data is segregated by client and project. Data is stored for the length of time agreed upon in the client contract, and Consilio follows proper data destruction policies at a project's end. Formal data destruction or transfer forms must be signed by clients before data is destroyed, and Consilio issues a certificate of data destruction after the data has been destroyed.

Asset Management: All equipment is tracked and controlled through Consilio's asset management policies. Chain of custody documentation and controls are followed for all client equipment and media. Client media is stored in secured and locked areas and only accessed by authorized data management personnel.

Certifications & Compliance

Consilio is certified for the ISO/IEC 27001:2013 and ISO/IEC 27701:2019 standards and HITRUST CSF V9.3, and meets all of their stringent requirements to appropriately handle sensitive data. All of Consilio's colocated data centers are either certified for ISO 27001 or have completed SOC 2 Type 2 audits. Consilio complies with ITAR regulations, EU-US and Swiss-US Privacy Shield principles* (still applicable in the US), the EU General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and many other data privacy regulations across the globe. Consilio's data center and office locations in the UK are also certified for the Cyber Essentials Plus scheme.

**Note: Although the EU-US Privacy Shield framework was ruled invalid by the European Court of Justice, Consilio will continue to honor all privacy-related contractual requirements entered into when the original framework was in place. If new applicable regulations are created to replace Privacy Shield, Consilio will comply with all applicable laws.*

Privacy

Consilio's privacy policies and practices follow and often exceed international best practices for data security. Our enterprise privacy structures and policies ensure that we meet the requirements of international and local privacy regulations, based on the location of each project and data. These include regulations such as ISO/IEC 27701, GDPR, HIPAA, ITAR, CCPA, and others like it.

Qualified data privacy officers oversee implementation of our privacy standards. Consilio's information classification policies ensure that all data is appropriately protected based on its sensitivity. Access restrictions to client data are always based on the client's request and adherence to local regulations and client contractual requirements.

Physical Security

Consilio's colocation data centers are certified for the ISO 27001:2013 standard or have completed SOC 2 Type 2 assurance audits, depending upon the data center location. Consilio has colocation data centers in various locations worldwide to address jurisdictional data security and privacy requirements of our clients. Consilio executes strict contracts and nondisclosure agreements with colocation data center operations vendors to ensure the security and confidentiality of our data and equipment.

Within the data centers, strict physical and logical security controls are in place to ensure Consilio's assets are properly segregated from other assets in the data center and that our clients' assets are properly segregated from each other. Consilio servers are physically isolated in dedicated Consilio IT equipment cages within colocation facilities. Only authorized employees from Consilio's IT team can physically access the server areas. Each entry into and exit from any Consilio data center server room is logged and traceable. Video cameras continuously record physical movement throughout the buildings and perimeter, and surveillance footage is retained in multiple locations.

Physical security measures at colocation data center facilities include:

- Perimeter security, including fences and entry gates.
- 24/7 security guards.
- Access-controlled doors to the facility and equipment rooms, including locks secured by:
    - Pin codes.
    - Biometric scanners.
- A segregated rack space and locked cage for Consilio IT equipment within the data center.
- CCTV surveillance and backup storage of the footage.
- A visitor management process that:
    - Prohibits entry of unauthorized personnel into the data center.
    - Requires visitors to be pre-approved and accompanied by authorized personnel when inside the data center.
- Environmental controls such as UPS, HVAC, fire suppression, and backup generators.

Data Security

Consilio's policies for handling client data ensure that data and devices are stored securely and protected from unauthorized access while in Consilio's possession. All client data is treated as confidential, whether the data includes personally identifiable information (PII), protected health information (PHI) or simply non-public information.

Physical and logical security controls include strict authentication controls, strong passwords, data segmentation, isolation of client data from other organization data, and role-based access based on the principle of least-privilege. Internal procedures for granting access to the client's project data vary based on the unique nature of Consilio's business engagement with the client, client contractual requirements, adherence to local regulations, and security considerations for the specific situation. Access to client data is only granted to those who have obtained proper authorization and require access to perform their job functions. Clients have full discretion about who is granted access to their data and projects.

Secure data handling policies are enforced throughout the entire lifecycle of an eDiscovery project, including maintaining a valid chain of custody for the data until it is returned to the client or destroyed. Projects begin with Consilio collecting the data, performing data intake and processing on our specialized systems, and performing document review on secure devices in Consilio's custody or the client's custody. When a project ends, the client can opt for Consilio to return data to the client or destroy the data (including physical media), which includes a certificate of destruction. Technical, operational, and management controls are deployed to ensure compliance to data security requirements throughout the data lifecycle.

Consilio does not comingle clients' data. We create virtual servers that are dedicated to a specific client and project within our secure technology infrastructure. We only store client data for the length specified in the client contract, and then data is destroyed or returned to the client, based upon client instructions.

Network Security

All internet-accessible systems are located in a DMZ network behind a secure firewall. All client data resides in the secure network behind a second identical firewall. Both firewalls are configured to allow only the bare minimum of access. No traffic is allowed from the internet directly into the secure network. Communication between these networks is encrypted using 256-bit SSL encryption to guarantee that no data (including login credentials) is ever transmitted in plain text over a public network.

Consilio's network security controls include the following:

1. All internet connected locations are protected by firewalls, intrusion detection system and intrusion prevention system (IDS/IPS) infrastructure, and security information and event management (SIEM) software deployed in a fully redundant configuration. All traffic entering or leaving the Consilio network must traverse through controlled secure entry points.

2. Network security protocols such as BGP, MPLS, and IPSec are enabled to ensure network traffic is securely traversing within the Consilio network, server, and end-user segments. Consilio has segregated systems for networking and server class equipment for web/web services, database, and storage activities.

3. Strong authentication controls (e.g., strong passwords, multifactor authentication, data segmentation, role-based access) are enforced in Consilio's network environment to ensure appropriate access controls for client data. Internal authentication is performed against an Active Directory LDAP server.

    a. Unique user IDs and strong passwords are required for all users.

    b. Consilio uses a third-party tool to enforce compliance with password policies for Active Directory accounts. All vendor default passwords/accounts are required to be changed or removed upon first use.

4. Consilio uses standard encryption algorithms, such as AES, to protect data at rest (AES-XTS 256-bit certificate encryption) and in transit (TLS 1.2 and 1.3 only, 128-but/256-bit ciphers for symmetric encryption algorithms). Cipher suites are configured per Mozilla's Intermediate compatibility standard.

5. All Consilio systems are hardened in accordance with Consilio's baseline hardening policies to ensure unused ports are locked and connection strings are established with known servers and services only.

6. All Consilio servers and workstations have approved antivirus and anti-malware software installed. Advanced endpoint threat detection software and mobile device management solutions are implemented on all Consilio endpoints.
7. All changes related to information technology and application development are properly reviewed and authorized before being implemented into a production environment.
8. Application and network vulnerability assessments and penetration tests are performed regularly. Internal and external vulnerability scans and penetration testing are carried out biannually by a trusted third-party team and more frequently by internal teams.
9. Consilio's software development life cycle process includes a secure development framework. Development, testing, and production environments are separated to ensure the security and integrity of our systems and data.

Document Review

Consilio offers secure document review services onsite and remotely through our secure virtual review (SVR) platform. All users on a Consilio document review project (whether onsite or remote) are required to authenticate to Consilio's secure virtual environment, which is segregated in its own network configuration with strict security controls:

- Document review systems are placed in a segregated VLAN environment.
- Review facilities are provisioned with secured, locked-down thin client systems that are configured to only allow software utilities that are specifically required for that document review project setup.
- Consilio's secured document review systems restrict web content, printing, and email capabilities, in accordance with client project specifications.
- Consilio's secured document review systems do not allow use of Wi-Fi, instant messaging tools, removable media drives, or printer access, unless specifically requested by the project client or for secure virtual review.
- User-based group access policies are applied to document reviewer accounts to restrict access to only authorized document review systems.
- Role-based access control policies are applied to document reviewers and include multifactor authentication if the client requests it.

Personnel

All Consilio employees and contractors must complete background screening before being hired. Consilio personnel are required to:

- Sign nondisclosure and confidentiality agreements during personnel onboarding.
- Complete information security awareness training during onboarding and annually.
- Agree to follow Consilio's security policies.
- Maintain training relevant to their job duties.
- Be qualified for their positions and maintain applicable educational qualifications throughout employment.

Consilio
consilio.com

Vendor Risk Management

Consilio's vendor risk assessment policy requires that Consilio vendors and third-party suppliers be properly vetted and approved before engaging in work for Consilio and periodically undergo security audits by Consilio. Consilio's contractual agreements with vendors include confidentiality clauses that protect Consilio and its clients' information. Consilio performs vendor risk assessments at least annually.

Consilio also monitors our vendors for emerging supply chain vulnerabilities and follows up with them whenever new issues are identified.

Incident Management

Consilio's incident management policy ensures that we take proactive measures to prevent and report privacy and security incidents and mitigate their effects. Consilio discloses any incidents involving client data within the timeframe required by the client contract. Consilio incident response procedures also cover internal escalation protocols, including the process for escalation and notification to management, clients, and external governing bodies, as applicable.

Consilio's incident response team is supplemented by a 24/7 security operations vendor that has the ability to take immediate action in emergency situations. The vendor can isolate problem endpoints/users immediately after a potential incident is indicated, which helps prevent the effects of the incident from spreading further from a potentially compromised endpoint.

Disaster Recovery and Business Continuity

Consilio's disaster recovery and business continuity policies require that Consilio prepare for disaster scenarios that could disrupt business operations at our data centers or offices. Plans cover events such as natural disasters, pandemic scenarios, utility disruptions, personnel shortages, and other events that could affect staffing or business resources.

Consilio's disaster recovery plan covers stages of our initial response and assessment after a disaster, mobilization and communication with our staff and clients, restoration of services, validation of proper functioning, business resumption, interim operations, and the return to normal operations. Consilio's disaster recovery and business continuity plans address the associated management of risk, legal and regulatory requirements, and how to resume serving our clients after a disaster.

Consilio's documented recovery time objectives vary for each IT asset and application. Specific recovery time objectives for certain applications, data, or projects can be obtained from the Consilio client services representative for each project. Recovery time objectives are documented and tracked for all assets and applications and are tested in Consilio's annual disaster recovery and business continuity tests.

Data Backup

Consilio's data backup policy requires that we perform a combination of data replication, daily incremental backups, and weekly full backups of critical data. Consilio's primary and secondary data center facilities are located at least 25 miles apart to ensure that disaster at one data center would not render the secondary data center inoperable.

Ready to Learn More?
Visit consilio.com/complete or email info@consilio.com