ENVESTNET
Yodlee

Global Security FAQ

(Frequently Asked Questions)

An Introduction to the Yodlee Information Security Program

Version 5.0

Envestnet and Yodlee are different companies, but Yodlee follows the Envestnet information security program in addition to Yodlee specific measures, which are identified in this document.

Envestnet

Does Envestnet have a Risk Management Program?

Envestnet has enacted a comprehensive risk management program designed to intelligently focus resources and efforts on the assessment, monitoring, and management of our corporate and information security risk profiles.

The Risk Management program consists of formal risk assessments at the organizational and product levels. In addition, risk management is incorporated in all facets of our processes, including integration with application development, data center operations, and internal security management. Envestnet's company-wide Enterprise Risk Management Program (ERM) ensures that the necessary information is available for our Executive Management team and board to make effective risk-based decisions.

The Envestnet ERM is standards-based, incorporating ISO (International Organization for Standards), COSO (Committee of Sponsoring Organizations of the Treadway Commission), and FFIEC (Federal Financial Institutions Examination Council) requirements, as well as maps to the Basel Committee's Risk Management Principles for Electronic Banking.

Information Security Program

What is Envestnet's Information Security Program?

Envestnet has adopted a risk-based information security policy framework at the enterprise level. Envestnet is committed to protecting all information accessed, processed, stored, or exchanged, from unauthorized access, use, modification, disclosure, or destruction, by implementing controls defined to meet organizational objectives. Envestnet has a comprehensive information security management program and policy framework that leverages elements from NIST (National Institute of Standards and Technology), CSF (Cybersecurity Framework), NIST Standards, ISO 27001, and CSA (Cloud Security Alliance).

Is management responsible for the Information Security Program?

While the Envestnet culture is based on individual responsibility for security at all levels, the Envestnet Information Security team is responsible for defining, implementing, and monitoring the Information Security Program. The Information Security team operates under the supervision of the executive-level Security Oversight Committee and the board-level Compliance and Information Security Committee.

What is the Envestnet Information Security team?

The Envestnet Information Security team is a dedicated independent security, privacy, risk, and compliance function in the Envestnet business unit. It reports to Envestnet's executive management and has dotted line reporting to Envestnet's global compliance and security leadership. The Information Security team is organized around Four primary functions:

- Audit, Risk, and Compliance
- Cloud Security Operations
- Application Security
- Security Operations Centre

Each group is staffed with engineers, architects, and analysts with responsibilities relating to their primary role, while also acting as backup for each other. By working closely with other Envestnet groups, the Information Security team drives security, privacy, risk management, and compliance throughout the organization.

What is the Information Security Management Committee (ISMC)?

The Envestnet Information Security Program is directed by an executive committee called Information Security Management Committee (ISMC). This committee is comprised of Executive and Senior Management. The ISMC meets quarterly to review the security program, as well as to approve policies and to address governance matters.

What is the Board's Role in Security?

The Envestnet Compliance and Information Security Committee of the Board of Directors is responsible for all security and risk matters, except for Financial Statement Risk, which is addressed by the Audit Committee. This committee receives regular reports from the Information Security team on audits, security issues, changes in risk postures and regulatory matters. The Compliance & Information Security Committee selects Envestnet's independent security assessors and reviews their reports.

Does Envestnet have documented security policies and procedures?

An essential component of the Envestnet Information Security Program are the policies, procedures and standards that define our security controls. The Information Security team is responsible for these policies and for working with our Operations, Customer Care, and other groups to craft procedures that allow them to accomplish their tasks while protecting our users' data. Security policies are reviewed and approved by the Security Oversight Committee annually, or whenever material updates are made during the year. A current listing of our library is available upon request.

Does Envestnet have a Security and Privacy Awareness Program?

Envestnet has security, privacy, and compliance awareness embedded in all aspects of employee communications, including:

- Non-Disclosure and Confidentiality agreements
- Setting expectations of conduct in the Employee Handbook
- Mandatory security and privacy awareness training and testing upon hire
- Secure coding and build procedure
- Ongoing awareness training programs
- Feedback from monitoring systems

The Information Security team is responsible for developing, implementing, and maintaining this program.

Does Envestnet have an Incident Response Program?

The Information Security team maintains a formal program for Security Incident Reporting and Security Incident Response. Policies define our standards and guidelines of the program, with documented procedures that detail handling, communication, and reporting to clients, regulators, and law enforcement. Envestnet's Security Incident Response Program complies with regulations and standards, such as FFIEC and PCI DSS (Payment Card Industry Data Security Standard) and is aligned with good industry practices such as NIST and CERT (Community Emergency Response Team).

Personnel Security

Does Envestnet vet employees?

All employee and contractor candidates, regardless of role, are subject to a thorough background investigation prior to employment. This investigation includes education/professional qualification, employment verification, criminal record verification, address verification and drug screen.

Do employees sign confidentiality agreements?

All personnel sign non-disclosure and confidentiality agreements as part of on-boarding. These agreements ensure our personnel are made aware of Envestnet's obligations for security, privacy, and compliance.

Envestnet personnel annually re-affirm their compliance to our Acceptable Use Policy and our Confidentiality Agreement.

Is there formal termination and role change procedure?

Formal procedures for employee separation and role changes are defined to coordinate the applicable tasks between HR, Information Security, Internal Audit and the Envestnet IT (Information Technology) department. The procedures establish protocols for scheduled and immediate terminations. The Information Security team in conjunction with Internal Audit team conducts quarterly entitlement audits to verify that accounts of terminated personnel are either disabled or deleted.

Physical Security

How are sites secured?

At our offices, all employees must always carry and display their badge. All visitors must present themselves at reception to sign in and receive a visitor badge. Visitors are escorted while on site and must surrender their badge when they leave.

All offshore facilities from which platform operations are supported will be in secured work bays with standard controls.

Data Centers have additional access controls with biometric access, key cards, and security staff on-duty 24/7. Access is strictly limited to pre-authorized Envestnet personnel with a data center cardkey.

Vendor Risk Management

How are critical vendors managed?

The Vendor Risk Management Program ensures new vendors / service providers are selected and assessed by the stakeholders using a formal risk-based formula. They are assessed based on contractual agreements; financial, security and privacy due diligence; third-party attestations; and on-site visits.

Existing vendors and service providers are regularly reviewed, with ongoing management oversight for our most critical service providers. Envestnet's vendor risk evaluations are aligned with financial industry standards and supervisory guidelines.

Shared Assessment Vendor Risk Management Maturity Model Reports on key vendors, such as data center collocation providers, are available for client review.

Business Continuity Program and Disaster Recovery

Does Envestnet have a Business Continuity Program (BCP)?

Envestnet has a formal Business Continuity Program that encompasses all functions and sites. We conduct business impact analyses upon significant changes to our environment or personnel, and at least annually.

Does Envestnet test their BCP and DR?

Envestnet conducts a variety of tests throughout the year to ensure that our BCP and DR are designed and operating effectively.

Does Envestnet consider pandemic planning as part of their BCP?

Pandemic planning is part of our BCP and is updated to track current pandemic threats.

Does Envestnet test their DR Plan?

Envestnet conducts regular tests of our internal DR as well as supports annual testing with clients of their DR option.

Change Control

How does Envestnet perform Change Management?

The Change Management program is a formal and rigorous ITIL-based methodology for requesting, testing, approving, and promoting changes to our Production and Stage Environments. The Information Security team reviews and approves any critical changes to infrastructure or application.

Does Envestnet carry cybersecurity insurance?

Envestnet maintains cybersecurity insurance coverage as part of our comprehensive financial risk control program. While the exact providers, structure and limits are confidential, our insurance coverage is regularly reviewed and approved by our Board and auditors to ensure adequate protection for our current and anticipated exposures

Does Envestnet have a Security Operations Center?

Envestnet has deployed a layered monitoring infrastructure that incorporates data from point security solutions, monitoring tools, discovery scans and SIEMs (Security Incident and Event Monitoring) to produce a threat-derived correlated real-time view of our entire security architecture. This view is presented in Envestnet's custom Security Dashboard, which provides risk data visualization to all internal stakeholders, with a granular visibility to the asset, alert, or user level. The Security Dashboard is continuously monitored by Envestnet's 24/7 Security Operations Center (SOC). The SOC has run book procedures and SLAs (Service Level Agreements) for alert handling. SOC also reviews security advisories from vendor and third-party sources of threat information, risk assess them for the Envestnet environment and recommends suitable action as applicable.

Does Envestnet report breaches and incidents to

stakeholders?

The SOC and Information Security function ensure incidents and breaches are reported to the relevant stakeholders per defined internal processes based on specific contracted parameters.

Reportable issues will be handled per the applicable federal, state, territorial, or provincial data breach notification requirements.

Does Envestnet have data leakage prevention mechanisms?

Envestnet has deployed a DLP (Data Leakage Prevention) tool between the Production and Corporate environments to prevent the transfer of sensitive data from Production. Additionally, the Information Security team has commercial DLP tools to perform regular scans of the corporate environment.

Yodlee

How does Yodlee handle user data privacy?

Yodlee's Privacy Program is aligned with global privacy regulations, standards, and best practices. It is designed and operated to comply with applicable requirements for the regions in which we do business. In addition to compliance with U.S. federal and state regulations, Yodlee's privacy program has received third-party certification with US-EU and US-Swiss Privacy Shield as well as APEC (Asian Pacific Economic Cooperation) Cross-border Privacy Rules.

For Asia, Africa, Australia, and New Zealand, we adhere to applicable aspects of banking rules, privacy regulations, and consumer protection requirements. We consistently monitor new privacy regulations and programs to ensure we are meeting both the spirit and the letter of our clients' consumer protection requirements.

Does Yodlee adhere to any other global data protection laws?

Yodlee has operations in the U.S., Canada, Europe, APAC region, as well as in South Africa. Yodlee adheres to the prudential, consumer protection, and privacy regulations for all regions in which we operate. Yodlee tracks developments in new regions for any data protection requirements and actively engages with the regulators of the regions to ensure compliance.

Independent Assessments and Internal Audit

Does Yodlee have SOC 2 Attestation?

Yodlee conducts an annual SOC 2 Type 2 engagement, and the assessment report is available to clients and prospects under NDA (Non-Disclosure Agreement). The examination is conducted by an independent audit firm. The Trust Services Criteria in scope of the examination include security, availability, processing integrity, confidentiality, and privacy.

What third-party audits does Yodlee comply with?

In the United States, Yodlee is examined under the FFIEC Supervision of Technology Service Providers guidance. We receive a multi-agency examination by U.S. Federal Banking Agencies. The Report of Examination is available to charted financial institution clients via the OCC Western Region.

Internationally, Yodlee is not directly supervised by any other country's banking regulations. As an active partner in those financial ecosystems, we engage with our clients and their regulators, to ensure that our services are operating with respect for local requirements to enable our clients to comply with applicable regulations and standards for security, privacy, and vendor risk management.

Is Yodlee PCI certified?

Yes. Yodlee is PCI-DSS 3.2 certified as a Level One Service Provider. Our certification status can be viewed at:

•https://www.visa.com/splisting/searchGrsp.do

Are Yodlee's assessments available for review?

Yodlee's assessments are available to direct Yodlee clients and to prospects under NDA.

In the case of indirect clients, our Channel Partners conduct comprehensive due diligence of Yodlee's services and operations to ensure they meet the exacting standards that their clients expect from them.

Does Yodlee perform internal audits of its controls?

Yodlee has defined a comprehensive audit program that touches on the effectiveness and efficiency of every critical control. The Yodlee Audit team performs entitlement audits, technical audits and process audits following a published risk-based schedule. The audit program also defines detailed procedures for conducting each audit area. The audit program is vetted by our independent auditors and regulatory examiners.

Infrastructure Security

What is Yodlee's Infrastructure Security Program?

Yodlee follows industry best practice guidelines in the design and implementation of our infrastructure security program. We use zones to separate our Production, Staging, Development, Corporate and specialty networks from each other with access control devices between each zone. We further segment networks within each zone to apply granular security and audit controls appropriate to each function. Other key controls include:

- Central Bastion Hosts
- Multi-factor Authentication
- Resilient and Redundant Infrastructure
- Data Encryption
- Vulnerability Management
- Centralized Security Incident and Event Management (SIEM)
- Secure VDI Limiting Data Movement
- Layered Security Zones
- Enterprise Antivirus Management
- IDS/IPS Monitoring
- DDoS (distributed denial of service) Monitoring

Does Yodlee employ public cloud-based solutions for its aggregation services to clients?

No. The core services of the Yodlee Platform are delivered from our colocation data centers. We do use Amazon Web Services (AWS) for scalable processing and delivery of some data services. For these use cases, we employ private VPCs (Virtual Private Cloud) and conduct comprehensive risk assessments to identify and deploy the necessary controls for each type of service.

How does Yodlee conduct patch and vulnerability management?

Yodlee monitors mailing lists from vendors, the open-source community and industry partners such as FS-ISAC (Financial Services Information Sharing and Analysis Center) and InfraGard, which provide notification of new vulnerabilities.

An automated monitoring script checks the CVE (Common Vulnerabilities and Exposures) and NVD (National Vulnerability Database) sources for recently published vulnerabilities in the third-party components and libraries used for Yodlee applications.

Once a reported vulnerability has been identified and confirmed, the Information Security team conducts a formal review of the applicable patches provided by the vendors. Per Yodlee policy, vulnerabilities must be patched or otherwise remediated (i.e., compensating controls) as soon as possible and no later than 30 days for critical or high priority issues.

Data Governance and Security

What data is collected by the Yodlee Platform?

While the Yodlee Platform connects to a variety of financial institutions and related data sources, the information we may collect to power our services broadly falls into four categories:

- Identity: name, address, tax identifier, email, and phone
- Account: institution or issuer, access credentials, type (e.g., savings, credit card), identifier/number, balance, APR
- Transaction: type (debit, credit), date, amount, description, method (e.g., credit card, direct deposit) and, in case of spend, merchant information
- Commercial: data such as terms, derived content or data provided under a fee agreement

Does each client have a dedicated environment?

The Yodlee Platform is a shared product platform. Data is housed on the same platform, but it is kept logically separated. All clients have a Master Key, and every end-user is assigned a member id and every account has an account ID.

Accordingly, segregation of client data is implemented at multiple levels with no possibility of cross-account access.

Who at Yodlee has access to Client facing systems?

Yodlee follows the principle of least privilege for all entitlement systems. We implement this using role-based access control and enforce it in our production and stage environments using a technical privilege management system. This system ensures that Yodlee personnel have the entitlements they need for their role, but only those entitlements. All access is 100% keystroke and session logged, so the Information Security team has full audit coverage of all activities. All security logs are integrated with SIEM (Security Incident and Event Management) solution hosted in Yodlee and retained for 52 weeks (about 12 months).

These logs feed our monitoring tools so we can detect as well as prevent unauthorized access attempts from our personnel.

Does Yodlee encrypt data at rest?

Yodlee encrypts sensitive user data in our database using AES 256 (Advanced Encryption Standard) and keeps this data in ciphertext form in the data flows until necessary to decrypt for use. Yodlee uses a FIPS 140-2 (Federal Information Processing Standards) compliant network-attached hardware security module (HSM) for hardware-based keys management. Yodlee personnel does not have access to the hardware-based keys. Application access is via internal API (Application Programming Interface) calls from authorized IP addresses and requires certificate-based authentication with the HSM appliances' built-in CA (Certificate Authority). Administrator activities on the HSM require two-person controls.

Does Yodlee encrypt data in transit?

Yodlee's data security policies ensure that all sensitive data is encrypted in transit using a 256-bit key software encryption. Yodlee uses TLS (Transport Layer Security) for encrypting the data on the wire for all external interactions and most internal connections within the data flow.

How long is client data retained?

User data is retained until deletion is triggered by the client via API or user written request or until the client is decommissioned. Certain regulated data is required to be held for a period as required by law.

Does Yodlee use user data for non-production testing and development?

No. Yodlee does not use user data for testing purposes in non-production environments. Instead Yodlee uses in-house developed synthetic data generation tools for non-production test data. Per Yodlee's Security Policy, user data is always required to be stored only in the Production environment.

Layered preventive and detective controls prohibit user data movement outside the secure production environment.

Application Security

How does Yodlee manage software development lifecycle?

The Software Development Lifecycle (SDLC) process at Yodlee includes normal software procedures like requirement analysis, functional and architectural design, development, testing, deployment, branching of code, patches vs. new development, etc. Impact analysis is done as part of a feasibility study as well as the functional and architectural design stage. GitHub (a web-based version-control and collaboration platform for software developers**)** is used for source code management. Releases are managed using internal automation tools. The Quality Assurance team then carries out testing of new enhancements and does regression testing to ensure that existing features are not affected by the deployment of new enhancements before deploying to production. Yodlee's release cycles upgrade the platform with the latest versions uniformly across all installations, four times per year. The SDLC process at Yodlee has been designed around secure development practices:

- Yodlee's application development process includes Open Web Application Security Project (OWASP) threat modeling.
- Yodlee has published a secure coding and awareness guide for all developers based on OWASP. As part of Yodlee's SDLC, static and dynamic scans are performed prior to each release.
- Information security is integrated into the software development process.
- Developers are required to follow the documented software procedures for development, testing, deployment,

branching of code, patches vs. new development, etc.
- For the Yodlee platform, Yodlee follows a quarterly release schedule for major enhancements.
- The standard application software patch release schedule is weekly, if changes are required.
- If a fix is required, depending on the severity, it will either be rolled out into a weekly patch or will be rolled into a future enhancement release cycle.
- Yodlee's network undergoes an annual penetration test by a third party. The test is based on OWASP Top 10 guidelines

What is Yodlee's Application Security Program?

The Application Security Program, run by the Information Security team, is a formal methodology integrated with the Yodlee Unified Process to apply security input, testing, and certification at all phases of the software development lifecycle. The Application Security function is an entirely independent team from the development staff and carries full veto power at every step of the process.

The program is human driven, aided by the leading application security products and tools in the industry. Security and privacy are built into our products from the specification stage and tested at multiple points up to and including release. Code cannot be released to production until the Information Security team signs off. Our Application Security Program includes:

- Driving enhancements to Yodlee products to incorporate evolving security features
- Reviewing all functional enhancements from compliance perspective
- Publishing secure coding standards
- Creating developer security training
- Performing manual and automated code reviews
- Manual and automated vulnerability testing
- Monitoring and continual protection by tracking
- Develops tools and monitoring profiles for security tools to automate security processes
- CVE/NVD listings for new vulnerabilities and threats
- Managing third-party assessments performed by external vendors or by our clients

Does Yodlee conduct penetration tests and code scans?

As part of the Application Security Program, static and dynamic code scanning, manual reviews, and multiple rounds of penetration testing are completed to test and certify the Yodlee Platform. Additionally, third parties perform annual application penetration tests on all internet facing applications.

Does Yodlee conduct static code analysis?

Our application security program relies on manual testing and several in-house tools with a comprehensive risk model to filter out false positives related to the lack of context provided by some of the tools. Yodlee has incorporated binary static analysis in the application certification process at key points in our methodology using custom rules for our specific code base. We have integrated these tools with our code vault so that automated static analysis is conducted on code as it is checked-in by developers. These analyses generate reports which are sent to the application security team for review with feedback provided to the developer in the form of bugs or other corrective actions.

The platform code base comprises all aspects of our service offering, is incredibly complex and as such requires significant context to understand and assess it. Due to the complexity of the code, we do not make it available for any one client to conduct a static analysis nor do we use third-party vendors who offer "static analysis as a service" type engagements.

We have run multiple pilots with such vendors and while the results are sometimes informative, they have not discovered enough or type of risk, vulnerabilities or other issues that justify the cost, burden, and risk of IP disclosure. The reports from these pilot engagements are not suitable for client review due to false positives, errors, and misleading issues due to complexity and context considerations.

Does Yodlee monitor for web application attacks?

Yodlee uses an industry standard web application security system to monitor all inbound application traffic. This monitoring includes the API calls that originate from your server/systems. If we detect repeated attack patterns (such as XSS, SQL Injection, etc.), we blacklist the originating IP from all communication protocols.