Security FAQ

An Introduction to the Envestnet | Yodlee Information Security Program

January 2017

Risk Management Program

Does Yodlee have a Risk Management Program?

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

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

The Yodlee ERM is standards-based, incorporating ISO, COSO and FFIEC requirements, as well as maps to the Basel Committee's Risk Management Principles for Electronic Banking.

Information Security Program

What is Yodlee's Information Security Program?

The Yodlee Information Security Program (ISP) is a comprehensive program of risk-driven policies with supporting procedures, guidelines, and audit. The ISP covers all aspects of the Production, Development, Staging and Corporate environments as well as vendor relations, BCP, and personnel management. The Information Security Program ensures a dynamic and robust controls environment for all of Yodlee's operations.

Is Management responsible for the Information Security Program?

While the Yodlee culture is based on individual responsibility for security at all levels, the Yodlee Security Office (YSO) is ultimately responsible for defining, implementing and monitoring the Information Security Program. YSO operates under the supervision of the executive-level Security Oversight Committee and the Board-level Risk Committee.

What is the Yodlee Security Office (YSO)?

YSO is a dedicated security function, headed by a Senior Vice President, who reports directly to the CEO. YSO is organized around three primary functions:

- Information Security
- Infrastructure Security
- Application Security

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 Yodlee groups, YSO is able to drive security, privacy, risk management and compliance throughout the company.

What is the Security Oversight Committee (SOC)?

The Security Oversight Committee is comprised of Executive Management and meets at least quarterly to review Yodlee's Risk Management and Information Security Programs, approve policies and to address security and risk matters.

What is the Board's Role?

A sub-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 YSO on audits, security issues, changes in risk postures and regulatory matters. This Committee selects Yodlee's independent security assessors and reviews their reports.

Does Yodlee have documented security policies and procedures?

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

Does Yodlee have a Security & Privacy Awareness Program?

Yodlee has security and privacy awareness embedded in all aspects of employee communications, beginning with required

- 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 procedures.
- Ongoing awareness programs.
- Feedback from monitoring systems.

YSO is responsible for developing, implementing and maintaining this program.

Does Yodlee have an Incident Response Program?

YSO 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. Yodlee's Security Incident Response Program complies with regulations and standards, such as FFIEC and PCI, and is aligned with good industry practices such as NIST and CERT.

How does Yodlee handle customer data privacy ?

Yodlee's Privacy Program is aligned with global privacy regimes, 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 US federal and state regulations, Yodlee's privacy program has received third-party certification with US-EU Privacy Shield and US-Swiss Safe Harbor Programs as well as the Asia Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CPBR) We consistently monitor new privacy regulations and programs to ensure we are meeting both the spirit and the letter of our and our clients' consumer protection requirements.

Does Yodlee carry Cybersecurity Insurance?

Yes, Yodlee maintains cybersecurity insurance coverage as part of our comprehensive financial risk control program. Our clients benefit from their contract's indemnifications of security, privacy and compliance related issues. These

indemnifications provide assurances that Yodlee stands behind our commitment to keep your, and your customers', data protected. As a public company engaged in global operations, it is prudent for us to maintain insurance coverage(s) that enable us to support these indemnifications should a triggering event occur. 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 protections for our current and reasonably anticipated exposures.

Independent Assessments and Internal Audit

Does Yodlee have an SSAE16 or SOC2?

Yodlee uses the *Shared Assessment Program* in lieu of the SSAE16. The Shared Assessment consists of two parts. The first is a Standard Information Gathering Questionnaire that Yodlee uses as a controls selfassessment.

The second is a set of Agreed Upon Procedures executed by a qualified third-party. Both the SIG and this Report of Agreed Upon Procedures are available to Yodlee's direct clients. Summaries are available to institutional clients of our Partners. The Shared Assessment is recognized as a more comprehensive and objective assessment than an SSAE16 for financial industry service providers as it maps to ISO27002, FFIEC, and PCI. It also tracks directly with the requirements of our clients' vendor security programs.

Do the banking regulators examine Yodlee?

In the US, Yodlee is examined under the FFIEC Supervision of Technology Service Providers guidance. We receive a multi-agency examination, with the OCC as Agency-in-Charge.

Internationally, Yodlee is not directly supervised by any other country's banking regulations. However, as an active partner in those financial eco-systems 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?

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

- http://www.visa.com/splisting/
- https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/service-providers-need-to-know.html

Are Yodlee's assessments available for review?

Yodlee's assessments are available to direct Yodlee clients or 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 high standards that their clients expect from them. To further support them, Yodlee has provided them with a *Yodlee Compliance Package* to share with you that summarizes our audit and compliance programs.

Will Yodlee fill out a client's security questionnaire?

Yodlee treats the presentation of our security, privacy, risk and compliance programs as seriously as we take their operations. For this reason we put a great deal of effort into our

own due diligence package that we provided to our clients, including a quality review and management approval. We therefore decline requests for "one-off" questionnaires as they do not (cannot) receive the same level of attention. This is a requirement of our management and Board.

Does Yodlee perform internal audits of their controls?

Yodlee has defined a comprehensive audit program that touches on the effectiveness and efficiency of every critical control. Yodlee Security Office performs entitlement audits, technical audits & process audits. The audit calendar is a published schedule of audit activities for the calendar year. The audit program also defines the detailed procedures for conducting each and every audit area. The audit program is also vetted by our independent auditors and regulatory examiners periodically.

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 in order 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

Where is my data stored and accessed?

Yodlee has data centers in the US, Canada, UK Australia and India. Client data stays in the data center they've selected. Yodlee does not ship data cross borders. Data is accessed securely from our US and India facilities using secure access technologies to prevent accidental crossborder transfer or data leakage of sensitive data.

Who can access the data?

Yodlee follows the principle of *least privilege* for all entitlement systems. We implement this using role-based access control (RBAC) and enforce in our Production and Stage environments using a 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 YSO has full audit coverage of all activities.

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 Customer Data in the database using AES256 and keeps it in ciphertext form in the data flows until absolutely necessary to decrypt for use. Yodlee uses a FIPS 140-2 compliant network-attached hardware security module (HSM) for hardware based key management. Application access is via internal API calls from authorized IP addresses and

requires certificate based authentication with the HSM appliances' built-in CA. Administrator activities require two-person controls.

Does Yodlee encrypt data in transit?

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

Does Yodlee have a Security Operations Center?

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

Application Security

How does Yodlee manage SDLC?

Yodlee employs a formal software development lifecycle and Release Management process we call the Yodlee Unified Process (YUP). YUP is a hybrid waterfall/agile methodology for all development and product lifecycle activities. Ideation, BRD and FSD phases follow traditional waterfall processes as does release management. Coding follows the Scrum interactive methodology. YUP ensures input and visibility for internal and external stakeholders.

What is Yodlee's Application Security Program?

The Application Security Program, run by YSO, 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 AppSec function is an entirely *independent* team from the development staff and carries full veto power at every step of the YUP.

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 YSO 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, YSO uses static and dynamic code scanning, manual reviews and multiple rounds of penetration testing to test and certify the Yodlee Platform. Additionally external vendors and clients perform periodic penetration testing on the Yodlee application.

Does Yodlee conduct static code analysis?

Our application security program relies on manual testing and a number of tools (including Fortify and AppScan) with a comprehensive risk model to filter out false-positives related to the lack of context provide by some of the tools, such as Fortify. 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 Fortify 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. Fortify is also used to conduct static analysis as part of formal certification steps on the path to GA.

The Yodlee 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 a sufficient number 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 leading web application firewall to monitor all inbound application traffic. This monitoring includes the API calls that originate from your server/systems. If we detect repeated attack patterns (Like XSS, SQL Injection, etc.), we blacklist the originating IP from all communication protocols Personnel

Does Yodlee vet employees?

All employee candidates, regardless of role, are subject to a thorough background investigation by YSO prior to employment. This investigation includes credit checks, criminal records search, residence verification, verification of employment and verification of academic qualifications and certifications. Repeat investigations are conducted regularly during employment and anytime there is a cause for concern. The Yodlee Background Investigation Standards provides guidance for scoring candidates based on results and assigns a risk rating. HR and YSO give final approval for candidates.

Do employees sign confidentiality agreements?

All personnel sign non-disclosure and confidentiality agreements as part on-boarding. These agreements ensure our personnel are made aware of Yodlee's obligations for security, privacy and compliance with our Services and internally for our operations. Yodlee 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, YSO, and the Yodlee IT department. The procedures establish protocols for scheduled and immediate terminations. YSO conducts quarterly entitlement audits to verify that accounts of terminated personnel are either disabled or deleted.

Physical Security

How are sites secured?

Physical security is overseen YSO and managed by our local administration teams.. At our offices, all employees must carry and display their HID badge at all times. There are strict rules against tailgating. All visitors must present themselves at Reception to sign in and receive a Visitor Badge. Visitors are escorted while on the site at all times and must surrender their badge when they leave. Access to sensitive areas requires YSO approval based on job responsibility. The most sensitive areas have biometric access devices used in tandem with the HID badge reader.

At our Data Centers, access is only granted to necessary Operations and YSO personnel, who must be preapproved by YSO. Access to the data centers requires badge and biometric identification. An authorized Yodlee employee must accompany visitors to the Data Center.Also, visitors must sign in and show a government issued photo ID while on the site.

All Yodlee facilities have comprehensive video surveillance.

Vendor Risk Management

How are critical vendors managed?

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

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

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

Business Continuity Program & Disaster Recovery

Does Yodlee have a BCP?

Yodlee 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 Yodlee test their BCP?

We conduct a variety of tests throughout the year to ensure that our BCP is designed and operating effectively.

Does Yodlee consider pandemic planning as part of their BCP?

Pandemic planning has been part of our BCP since 2006 and is updated to track with current pandemic threats.

Is Disaster Recovery part of Yodlee's services?

Yodlee has formal DR programs for our internal services and our clients' applications. Our client DR options includes contracted RPO and RTO designed to map with our client's requirements. Your Yodlee Channel Partner or Customer Success Manager can provide you with the details of your particular implementation.

Does Yodlee test their DR Plan?

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

Change Control

How does Yodlee perform Change Management?

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