Ascendify

Ascendify Enterprise Security

Company, Application, Document, and Platform Security

Updated: September 2016

Ascendify has developed this security policy in recognition of the enterprise security requirements of our enterprise clients.

Security threats can come in many forms, including threats from inside an organization as well as external sources. The objective of Ascendify's security policies is to define the procedures, guidelines and practices for managing security in our environment. We have developed this policy to:

- Protect the privacy of customer data
- Ensure the availability of our service
- Enable the global scalability of our solution
- Deliver enterprise security policy compliance
- Protect the brand and reputation of our enterprise clients

We enforce our security policy with every new employee, perform routine security assessments, and evolve our policies to protect against perceived threats and changing system architecture. We recognize that the ultimate responsibility for information security rests with the Chief Executive Officer and I hold myself solely accountable for implementing the policy and related procedures at Ascendify.

Sincerely,

Matt Hendrickson

Matt Hendrickson
Chief Executive Officer
Ascendify Corporation

1. Company Security

a. Purpose

The objectives of Ascendify's Security Policy are to preserve:

- **Confidentiality -** Access to data shall be confined to those with appropriate authority.
- **Integrity -** Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability -** Information shall be available at the time when it is needed.

b. Policy Objective

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks managed by Ascendify by:

- Ensuring that all members of staff are aware of and fully comply with the relevant procedures described in this and other policies.
- Describing the principals of security and explaining how they shall be implemented in the company.
- Introducing a consistent approach to security, ensuring that all staff members fully understand their own responsibilities.
- Creating and maintaining within the company a level of awareness of the need for security as an integral part of the day-to-day business operations.
- Protecting information assets under the control of the company.

c. Scope

This policy applies to all information, information systems, networks, applications, locations and users of Ascendify or supplied under contract to it.

Responsibilities for Security
Ultimate responsibility for information security rests with the Chief Executive Officer of Ascendify, but on a day-to-day basis the Chief Technology Officer and senior executive department heads shall be responsible for managing and implementing the policy and related procedures throughout the organization.

Managers are responsible for ensuring their permanent and temporary staff and contractors are aware of:

- The security policies applicable in their work areas
- Their personal responsibilities for security
- How to access advice on security matters

All staff shall comply with security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

The Security Policy shall be maintained, reviewed and updated by the Chief Executive Officer. This review shall take place annually in December.

- Managers shall be individually responsible for the security of their physical environments where information is processed or stored.
- Each member of staff shall be responsible for the operational security of the information systems they use.

- Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.
- Contracts with external contractors that allow access to the company's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external company shall comply with all appropriate security policies.

d. Legislation, Compliance and Audits

Ascendify is obliged to abide by all relevant federal, state, and international regulations. The requirement to comply with this legislation shall be devolved to employees and agents of the Ascendify, who may be held personally accountable for any breaches of security for which they may be held responsible. Ascendify shall comply with the following legislation and other legislation as appropriate:

- Sarbanes-Oxley Act (SOX)
- Federal Information Security Management Act (FISMA)
- Health Insurance Portability and Accountability Act (HIPAA)
- The Data Protection Act (1998) UK
- Platform compliance with SAS70 Type II and SSAE 16

e. Policy Framework

Management of Security
At the board level, responsibility for enterprise security shall reside with the Chief Executive Officer. Ascendify's security officer or Chief Technology Officer shall be responsible for implementing, monitoring, documenting and communicating security requirements for the company.

f. Security Awareness Training

Information security awareness training shall be included in the new employee onboarding process. An ongoing awareness program has been established and will be maintained in order to ensure that staff awareness is refreshed and updated as necessary.

g. Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause. Information security expectations of staff shall be included within appropriate job definitions.

Security Control of Assets
Each IT asset (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

Access Controls
Only authorized personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

User Access Controls
Access to information shall be restricted to authorized users who have a necessary business need to access the information.

Computer Access Control
Access to computer facilities shall be restricted to authorized users who have business need to use the facilities.

Application Access Control
Access to data, system utilities and program source libraries shall be controlled and restricted to those authorized users who have a legitimate business need e.g. systems or database administrators.

Equipment Security
In order to minimize loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

Computer and Network Procedures
Management of computers and networks shall be controlled through standard documented procedures that have been authorized by the Chief Technology Officer.

Risk Assessment
Once identified, security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented security arrangements shall also be a regularly reviewed feature of Ascendify's risk management program. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

Security Event Response
All information security events and suspected weaknesses are to be reported to the Chief Technology Officer. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

Protection from Malicious Software
The company shall use software countermeasures and management procedures to protect itself against the treat of malicious software. All staff shall be expected to cooperate fully with this policy. Users shall not install software on the company's property without permission from the Chief Technology Officer. Users breaching this requirement may be subject to disciplinary action.

Removable Media
Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of Chief Technology Officer before they may be used on Ascendify systems. Such media must also be fully virus checked before being used on the company's equipment. Users breaching this requirement may be subject to disciplinary action.

Monitoring System Access and Use
An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

System Change Control
Changes to information systems, applications or networks shall be reviewed and approved by the Chief Technology Officer.

Intellectual Property Rights
The company shall ensure that all information products are properly licensed and approved by the Chief Technology Officer.

Business Continuity and Disaster Recovery Plans
The company shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

Reporting
The Chief Technology Officer shall keep the Board of Directors informed of the information security status of the company by means of regular reports and presentations.

h. Employee Security Training

All employees will complete Ascendify's security awareness training and agree to uphold the policy:

- If an employee identifies an unknown, un-escorted or otherwise unauthorized individual at Ascendify, they will immediately notify a company department head or executive.
- Visitors to Ascendify must be escorted by an authorized employee at all times. All visitors must be restricted to the appropriate areas.
- Employees are required not to reference the subject or content of sensitive or confidential data publically, or via systems or communication channels not controlled by Ascendify's. For example, the use of external e-mail systems not hosted by Ascendify's to distribute data is not allowed.
- Employees will keep a clean desk. To maintain information security they will ensure that data is not left on their desk unattended.
- Employees need to use a secure password on all Ascendify's systems as per the password policy. These credentials must be unique and must not be used on other external systems or services.
- Terminated employees will be required to return all records, in any format, containing personal information.
- Employees must immediately notify their manager in the event that a device containing data is lost (including mobile devices, tablets and laptops).
- In the event that an employee finds a system or process which they suspect is not compliant with this policy or the objective of information security they have a duty to inform their manager so that appropriate action can be taken.
- If an employee is assigned the ability to work remotely they must take extra precaution to ensure that data is appropriately handled.
- Employees must ensure that assets holding data are not left unduly exposed, for example visible in the back seat of a car.

2. Web Application Security

a. Purpose

The purpose of this policy is to define web application security assessments within Ascendify. Web application assessments are performed to identify potential or realized weaknesses as a result of inadvertent misconfiguration, weak authentication, insufficient error handling and sensitive information leakage. Discovery and subsequent mitigation of these issues will limit the attack surface of the platform. Ascendify services available both internally and externally as well as satisfy compliance with any relevant policies in place.

b. Definitions

- **Web Application -** Any service that accepts and processes HTTP/HTTPS protocols.
- **Major Release -** a significant application software update/code change such as a new interface design programming platform change.
- **Point Release -** An application software update/code change as part of the application lifecycle.

- **Patch Release -** An application software update/code change that addresses a bug or flaw.

c. Scope

This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at Ascendify. All web application security assessments will be performed by delegated security personnel either employed or contracted by Ascendify.

d. Policy

Web applications are subject to security assessments based on the following criteria:

- **New or Major Application Release -** will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.
- **Third Party or Acquired Web Application -** Will be subject to full assessment after which it will be bound to policy requirements.
- **Point Releases -** will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
- **Patch Releases -** will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.
- **Emergency Releases -** An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Chief Technology Officer or an appropriate manager who has been delegated this authority.

e. Risk

Security issues that are discovered during assessments will be mitigated based upon the following risk levels:

- **High -** Any high risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.
- **Medium -** Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.
- **Low -** Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of **Medium** risk level or greater.

f. Security Assessment Level

- **Full -** A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on industry best-practices. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.
- **Quick -** A quick assessment will consist of a (typically) automated scan of an application for the top ten web application security risks at a minimum.

- **Targeted -** A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

g. Exemptions

Exemptions to the need for a security assessment will be made by the Chief Technology Officer or delegated manager based on risk and criticality of needed application changes/functionality/architecture. Exemptions will assume the associated risk and will be documented as required by the change control policies.

h. Responsibilities

Engineering will be responsible for web application scoping, assessment, determination of discovered issue risk, and reporting to Project Management and application stakeholders. Project Management and application stakeholders will be responsible for the appropriate assessment scheduling and remediation efforts based upon assessment findings and Security Engineering recommendations.

i. Enforcement

Web application assessments are a requirement of the change control process and are required to adhere to this policy unless found to be exempt. All application releases must pass through the change control process. Any web applications that do not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the Chief Technology Officer.

3. Document Security

Ascendify has responsibility for safeguarding the confidential information with which we have been entrusted as an organization.

a. Hard and Soft Copies of Confidential Documents

All hardcopy confidential documents used by Ascendify are stored in a secured area accessible to only those employees whose job function requires them to handle such documents. A secured area includes a locked drawer, cabinet, or room. Access to these areas are controlled and monitored.

All electronic confidential documents maintained by Ascendify are safeguarded against possible misuse by storing these documents in a secure, password-protected area of Ascendify's network. Documents that are marked Confidential are stored in a CONFIDENTIAL file/folder that is setup for each client. Only those employees that require access will have the proper permission to access these folders. If Confidential documents are received by Email, then documents are saved to the secure sections of Ascendify's network and the email is immediately deleted. Forwarding of emails that contain Confidential information is prohibited unless the aforementioned secure method for sharing documents is unavailable.

b. Disposal and Destruction

Following the completion of any project where Confidential information was required, Ascendify’s project managers will delete the folder marked Confidential on the network to ensure that any/all confidential information and documents are removed. All hard-copies are also destroyed.

4. Platform Security

Ascendify's SaaS application was built on Amazon Web Services (AWS) to deliver a highly scalable cloud computing platform with high availability and reliability. In order to provide end-to-end security and end-to-end privacy, AWS builds services in accordance with security best-practices provides appropriate security in

those Services, and documents how to use those features. Ascendify uses these features and best-practices to architect an appropriately secure application environment. Together, Ascendify and AWS enable our customers to ensure the confidentiality, integrity, and availability of their data, maintaining trust and confidence.

AWS Security and Compliance Center
http://aws.amazon.com/security/
https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf

SOC3 Report
https://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf

a. Reports, Certifications, and Independent Attestations

AWS has in the past successfully completed multiple SAS70 Type II audits, and now publishes a Service Organization Controls 1 (SOC 1), Type 2 report, published under both the SSAE 16 and the ISAE 3402 professional standards as well as a Service Organization Controls 2 (SOC 2) report. In addition, AWS has achieved ISO 27001 certification, and has been successfully validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). In the realm of public sector certifications, AWS has received authorization from the U.S. General Services Administration to operate at the FISMA Moderate level, and is also the platform for applications with Authorities to Operate (ATOs) under the Defense Information Assurance Certification and Accreditation Program (DIACAP). We will continue to obtain the appropriate security certifications and conduct audits to demonstrate the security of our infrastructure and services. For more information on risk and compliance activities in the AWS cloud, consult the following:

Amazon Web Services: Risk and Compliance
http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf

b. Physical Security

Amazon has years of experience in designing, constructing, and operating large-scale data centers. AWS infrastructure is housed in Amazon-controlled data centers throughout the world. Only those within Amazon who have a legitimate business need to have such information know the actual location of these data centers, and the data centers are secured with a variety of physical controls to prevent unauthorized access.

c. Secure Services

Each of the services within the AWS cloud is architected to be secure and contains a number of capabilities that restrict unauthorized access or usage without sacrificing the flexibility that customers demand. For more information about the security capabilities of each service in the AWS cloud, consult the following:

Amazon Web Services: Overview of Security Processes
http://awsmedia.s3.amazonaws.com/pdf/AWS Security Whitepaper.pdf

d. Data Privacy

AWS enables users to encrypt their personal or business data within the AWS cloud and publishes backup and redundancy procedures for services so that customers can gain greater understanding of how their data flows throughout AWS. For more information on the data privacy and backup procedures for each service in the AWS cloud, consult the Amazon Web Services: Overview of Security Processes whitepaper referenced above. The AWS Security Center provides links to technical information, tools, and prescriptive guidance designed to help you build and manage secure applications in the AWS cloud. Our goal is to use this forum to proactively

notify developers about security bulletins. Such transparency is the backbone of trust between AWS and our clients.

5. Security Incident Reporting & Investigation Protocol

A security incident is an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information processed and maintained by Ascendify (data processor) as a service to our clients (data owner). This section outlines the procedures and protocols for notification of and response to a security incident or breach involving unencrypted electronic personal information.

a. Security Incident Reporting

In the event that an Ascendify staff member, client staff member, or any third party identifies a potential security incident involving a computer or network of computers, the computer(s) shall be immediately disconnected from the network, then shutdown. In all instances, Ascendify's Data Center Operations team will await further instructions from Ascendify's CEO and the impacted client's Legal/Compliance department prior to continued operation of the computer(s).

Any person who believes that a security incident has occurred, shall immediately notify Ascendify's CEO at matt@ascendify.com or 415-735-1605, Ascendify's VP Engineering, jason@ascendify.com or Ascendify's VP Operations, lauren@ascendify.com at 415-735-1601.

Upon notification of a suspected unauthorized acquisition of confidential information or personally identifiable information (PII), Ascendify shall promptly notify the Legal/Compliance department of any and all impacted clients.

The following information will be included in the notification:

a) Date of the breach.
b) Description of the breach.
c) Description of the information inappropriately accessed, collected, used or disclosed.
d) The steps taken to mitigate the harm.
e) Next steps planned and any long term plans to prevent future breaches.
f) Steps the client can take to further mitigate the risk of harm.
g) Contact information for the designated Information Security Officer at Ascendify.

b. Security Incident Investigation

Ascendify's designated Information Security Officer, VP Engineering, VP Operations and CEO will conduct an investigation into the security incident to determine whether there has been a security breach. All investigatory work will be documented within a **Confidential Information Security Incident Report** by the designated Information Security Officer.

High Risk Incident

- Loss or theft of computing devices or portable media.
- Detection or discovery of a program agent including, but not limited to viruses, worms, Trojan horse programs, keystroke loggers, rootkits, logic bombs, spam relays, remote control bots.
- Detection or discovery of unauthorized users, or users with privileges in excess of authorized

privileges.

- Detection or discovery of critical or widespread vulnerabilities, or misconfiguration that might lead to a compromise affecting the confidentiality, integrity or availability of the platform.

Low/No Risk Incident

- If no breach of data occurred or the amount of exposure or damage is minimal, then the incident will be classified as a Low/No Risk Incident.

c. External Notification to Affected Individuals

The designated Information Security Officer is responsible for controlling access to, and security of, the breached electronic equipment shall compile the list of the names of persons whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In coordination with the client, individuals whose information has been compromised shall be notified in the most expedient time possible, and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The breach notification will be sent by email or postal mail and provide a brief description of the security breach, a contact for inquiries, and helpful references to individuals regarding identity theft and fraud.

d. Root Cause and Prevention

Once the immediate security incident or threat has been mitigated, Ascendify will investigate the root cause of the breach. If necessary, this will include a security audit of physical, organizational and technological measures. As a result of this evaluation, the designated Information Security Officer will put into effect adequate long term safeguards against further breach. Policies will be reviewed and updated to reflect the lessons learned from the investigation so that future incidents may be prevented.

6. Frequently Asked Questions (FAQ's)

Ascendify has included the following answers to commonly-asked questions to help the security teams of our clients and prospective clients determine the security stance of the infrastructure behind the service we will be providing. Our goal is to be as thorough as possible when detailing the security controls and procedures in place at our company. Ascendify provides this comprehensive overview of our security program in order to reduce the amount of additional inquires and speed up the review process.

a. Provide a description of the services Ascendify will be providing?

Ascendify's Talent Platform is a comprehensive talent acquisition platform, which includes a talent community that helps take your recruiting to the next level. The platform can be configured to allow candidates to engage with the client's recruiters to source talent, hiring managers to evaluate candidates. Employees can refer their friends to the community through their social networks.

b. What type of information will Ascendify require to perform the service?

At a basic level, Ascendify collects and stores candidate information that is used to engage with the people that want to work for your organization. This information includes personally identifying information such as name, photo, address, phone numbers, email address and resume/CV information. Each of these fields can be required, not required or turned off by the client using the configuration settings in the Admin Console. Some clients choose to add their existing employees to the service so they may apply to jobs (internal mobility) and recommend jobs to people in their social network.

c. Will Ascendify connect with any of client's internal systems?

If clients have purchased Ascendify's Referrals module, then it is preferred that that we integrate via (Single-Sign-On) SSO so that employees of the organization can log in to the platform without a duplicate login so they may refer friends in their social networks to open positions. Also, it allows Ascendify to transfer hired applicants into its HRIS solution or other applicant tracking solution. Integration may also be considered as a future project if Referrals are not included in the initial rollout.

d. Does the vendor have a formal security program and resources assigned to it? Provide information regarding security policy, practices and procedures.

Yes. Ascendify has provided our security policy and identified the resources and policies within.

e. Describe the security controls that protect the network from external attacks and internal misuse of sensitive assets.

All data transmissions, both internally (server to server) and externally are SSL encrypted. All access to database servers are also firewall protected and password controlled using Amazon Security Groups. Thus, users must have the right IP access to access the data server and the right password to access the data.

f. How does Ascendify separate customer data?

Hardware and software configurations are designed to provide secure logical separations of customer data that permit each customer to view only its related information. Multitenant security controls include unique, non-predictable session tokens, configurable session timeout values, password policies, sharing rules, and user profiles. Ascendify uses logical separation to keep data from co-mingling and provides a consistent security layer built into the application that governs all access to the data, whether directly by a user or via an API.

g. Describe the patching and updating policies, procedures.

This is carefully described in Ascendify's Change Management Policy. In summary, we have a standard SDLC procedures for planning, developing and releasing updates/enhancements. "Patching" only occurs with P1 issues in emergency situations, which still leverages our automated release system. Refer to Ascendify's Change Management Policy for more details.

h. Describe the security controls that protect sensitive data (encryption, DLP mechanisms, access control, monitoring).

Any/all data that comes out of Ascendify's application or back-end servers is SSL encrypted. For the Talent Community, provided that the client provides Ascendify with a security certificate, then any/all data that comes out of Ascendify's servers are also SSL encrypted. For DLP, Ascendify has automated, nightly data replication to slave nodes in geographically dispersed regions (primary is Oregon, backup is Virginia) for both MongoDB and PostgeSQL data.

i. What is your backup policy, frequency and cadence?

Ascendify stores 15 days of immediate access daily backup and up to 90 days of retrieval with quarterly permanent backups.

j. How do you encrypt data at REST?

For disk-level encryption, Ascendify uses LUKS (Linux Unified Key Setup) which is the standard for Linux hard disk encryption. Additionally, special handling personally identifiable information (PII) is encrypted at the field level within the database.

k. What hashing algorithm is used for field level-encryption of passwords, social security numbers (if used), and other special handling personally identifiable information (PII)?

We encrypt passwords and any user-defined fields that are designate to collect special handling (PII) using SHA-256 encryption. Each field is hashed with a unique salt that is stored in the database and a system hash which is only stored on the server.

l. How do you dispose of personally identifiable information (PII)?

Upon end-of-life of an agreement, Ascendify removes (PII) from production servers (development, staging and production environments). Upon request, we can remove (PII) data from the last 15 days of daily backups.

The steps below are taken to ensure client data is inaccessible:

1. Overwrite client's data with 'junk' data
    a. Ensures the data cannot be recovered with data-recovery techniques even after the data has been removed
2. Remove all client data from our databases
    a. Prevents an attacker from gaining access to data because the data is no longer available
3. Remove all client files from our NFS servers
4. Remove the client's Talent Community
    a. People looking for jobs will no longer be able to visit the websites previously hosted
5. Remove any special configurations (if present) for the client in our environment (load-balancers)
    a. This is a cleanup step for Ascendify to keep our infrastructure in a maintainable state
6. Audit our data to ensure all data is up-to-date, and accurate
    a. Use quality assurance resources to ensure no steps were accidentally overlooked and ensure all data is removed properly

Data in Ascendify's quarterly backups are stored in Amazon Glacier which is highly secure, online file storage web service that provides storage for data archiving and backup. For an additional retrieval and data destruction fee ($10,000), Ascendify can extract all (PII) from back-up archives for each quarter where a backup was created (up to 2 years of historical data).

Ascendify

m. Describe processes or systems that monitor the infrastructure (logging, correlation, alerting).

Ascendify uses 3rd party monitoring services that include Amazon's Cloudwatch and Nagios and alerts come in various forms (email, phone, text). For low-level alerts, tests are run every 5 minutes and after 15 minutes of an error, then an email is triggered. For critical infrastructure, tests are run every few minutes and alerts are immediately sent via SMS and then escalated into a calling tree after 5 minutes of inaction. The first level of calling tree is the SysOps manager, the second level is the System Architect, and the third level is Executive Management. Calls are continuous until the alert is cleared.

n. Describe the company's application development process. What controls or processes are in place to avoid, detect and promptly remove vulnerabilities in applications.

Ascendify follows a standard SDLC with minor releases every three weeks and major new releases once per quarter. Before we release new functionality, we go through a feature review process, architecture confirmation, development, QA cycles and release procedures. At each stage, SysOps reviews for any potential vulnerabilities.

o. Describe operational controls in place. Audits, peer reviews, separation of duties, change management.

Either Ascendify's Engineering manager performs code reviews and or key, senior members of the engineering team perform peer reviews. Once code is marked Dev Complete, then the QA Engineering team reviews the new code and validates the code is working as expected and no ramification errors have been introduced. Each ticket is checked twice and validated before being pushed to Production. At each stage, SysOps review for vulnerabilities and potential threats.

p. Describe the physical controls that protect the environment.

We leverage Amazon's physical security. http://aws.amazon.com/articles/1697 Inside Ascendify's offices, we do not publish passwords or login credentials and keys are locked up in an alarmed building. Ascendify's employees are trained once per year on security per our security policy procedures.