SECURITY STRATEGY & POLICIES

Understanding How Swift Digital Protects Your Data

Table of Contents

Introduction

The Security of your data is one of our highest priorities.

Swift Digital diligently protects your proprietary and personal information as well as all data entrusted to you by your customers.

Effectively securing your business data is an essential prerequisite to successful use of our platform and services. To that end, this document explains how Swift Digital defends against attempts at unauthorized access, theft and other intrusions that threaten all online Software as a Service (SaaS) providers need to address.

We encourage you to thoroughly review our security standards and those of competitors, whether you are an active customer or a potential client performing technical evaluations of the product.

To discuss or receive enhanced details about our security commitments, write to Paul.Hodgson@swiftdigital.com.au

Security Infrastructure

Swift Digital data is hosted and managed through Amazon Web services (AWS) in the Australian Availability Zone (AZ)

AZ's are clustered together and are across multiple datacenters. AZ's are always separate buildings far enough apart that they won't be affected by the same fire, flood etc. This usually means that they aren't in the same colocation facility.

AWS Compliance whitepaper

https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf

AWS Security Whitepaper:

https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

Security Strategy and Policies

To maintain the safest possible cloud computing environment, Swift Digital's programming and security teams work together guided by the following principles:

- **Only deploy best-in-class facilities, hardware and software.** In addition to the physical and network security advantages of AWS critical assets are protected with firewall and intrusion detection software.
- **Constantly review and adapt to ever-changing threats. In addition to performing regular penetration tests** Swift Digital hires independent, certified companies to perform security penetration testing from login to data storage. We study the latest threats and counter measures, performing regular updates accordingly.
- **Need-to-know policies govern employee conduct.** To thwart costly and criminal intrusions, as well as to assure compliance with rules and best practices, Swift Digital employee and vendor access to our systems is restricted and monitored.

Operational Security

Swift Digital Suite operating system and applications are proprietary, built by our programming team using a hardened, enterprise version of Linux. The OS has been simplified to employ only the features and functionalities required by our processes, thereby eliminating numerous potential vulnerabilities.

Threat Management

Swift deploys server-level intrusion detection software. Data inflow is restricted to permitted file formats. We monitor systems for malware and DOS attacks.

Vulnerability Management

In addition to uninterrupted threat monitoring, Swift Digital personnel perform security penetration testing from login to data storage within our systems and the servers that host them. Protocols identify unusual traffic activity at all times and trigger responses to them. Identified weaknesses are corrected immediately.

Swift Digital values and stays abreast of advance warnings from government and cyber organisations. We believe vigilance and cooperation in the cloud-service community is critical to achieving a safe, secure and sustainable Internet.

We encourage and enable customers to perform Independent penetration tests on potential vulnerabilities. We facilitate these at times when services will not be impaired, generally on weekends after 12am. Testing by one or more customers will not impact system performance, nor will it be known by other customers.

Penetration tests do not reach any client data.

Encryption in transit at the application level

Data is encrypted as it flows across the network between the client and provider. All connections are via HTTPS. Using high level 2048 bit certificates.

SSL layer at the customer level

Clients are encouraged to further encrypt data between their Swift Digital account and their customers by having an SSL Certificate of their choice installed on their account to protect data such as registrations, subscriptions and survey responses

Encryption of Data at Rest

All data not moving through the networks are further protected through encryption of this data at rest.

Auditing and Monitoring

Live monitoring via Brocade, Splunk and New Relic is augmented by daily human reviews of our firewall and server log files for any suspicious activity.

Redundancy

Amazon's infrastructure has a high level of availability and provides customers the features to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact. Data center Business Continuity Management at AWS is under the direction of the Amazon Infrastructure Group.

Availability

Data centers are built in clusters in various global regions The Australian Data cluster is used by Swift Digital. All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area.

Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load balanced to the remaining sites.

Patch Management Policy

Our processes ensure that security patches are up to date. For the server network, AWS manages security patches and software updates. Their ISO quality and control certifications are comprehensive. Swift Digital operating environment requires us to focus on monitoring and implementing updates for Apache, MySQL and PHP.

Swift Digital's office PCs run valid and supported versions of Windows and iOS. Updates are automatic. These never store customer data.

Disaster Preparation & Recovery

Swift Digital's emergency readiness and response strategy features:

- **Separation of production and development servers.** By maintaining application source code, configuration and data backups in two locations, we can recover our systems in the unlikely event that the AWS data centres become unusable.
- DB is Multi-AZ. In the event of primary DB failure, it will failover to the secondary DB with minimal down time.
- Disaster recovery (DR) architectures Swift Digital deploy "hot standby" environments that enable rapid failover at scale. Hosted in two zones in Australia, we have a set of cloud-based disaster recovery services that enable rapid recovery for our IT infrastructure and data.

Our disaster response plans anticipate recovery from a failure of our primary database server (5 – 30 minutes) and outage of website servers (30 minutes to 2 hours).

Incident Response

Our primary objective in the event of a failure is minimising the business impact to our customers and us. To do that, we will immediately redeploy non-essential systems to provide resources to maintain business services.

In the event of a web server failure, our plans call for redeploying either our staging or network monitoring servers. These can take on this workload with minimal if any degradation in performance.

Physical Security

Server Environment

AWS's data centers are state of the art, utilizing innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.

Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these

privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWSemployees is logged and audited routinely.

Sophisticated alarm systems and closed circuit TV surveillance support 24x7 on-site security. These facilities are equipped with automated fire detection using Tyco Inergen Fire Suppression System in technical areas.

The server infrastructure is subject to constant monitoring and maintenance to ensure maximum uptime and reliability.

Monitoring the environment and performance of the data centers and their critical infrastructure is managed using sophisticated building management technology. This gives the on-site facilities team a single, integrated view every component of the physical plant and the cloud computing environment.

IRAP Compliance

AWS is IRAP compliant. An independent IRAP assessor examined the AWS controls including people, process, and technology to ensure they address the needs of the ISM. This assessment and Letter of Compliance is the basis on which a Certification Authority gains assurance to certify AWS infrastructure and provide a recommendation to the Accreditation Authority for appropriate use of the platform.

Client Data Security and Privacy

User Environments

Swift Digital systems and applications are secure for both stand-alone and workgroup implementations. Clients can scale their security to suit a single user, a small team, or workgroups of any size. Security can be enforced at the database level and feature level.

Data Ownership

Our clients own all rights, title and interest in the data we store, secure and manage for them. Secure exporting is enabled any time an account is active and in good standing.

PII Controls

Swift Digital takes seriously its commitment to protect the privacy of its customers' subscriber's data. For that reason, we classify our information assets into risk categories (high, moderate, low) for the purpose of determining who is allowed to access the information and what minimum security precautions must be taken to protect it against unauthorised access.

The data loaded into the Swift Digital Platform is at the discretion of the client and as such access to Personally Identifiable Information is under the direct control of the client. While extensive security controls are in place to prevent unauthorized access to PII data it is recommended that data in Swift is kept to the minimum amount required for the purpose of marketing and communications.

Access to Data is managed through the user management console and folder access layers.

This puts into place restrictions on which users have access to mail-house data to view or edit data.

These restrictions allow the client to establish their own specific PII Controls.

An example of a PII Control policy matrix in terms of Swift Digital may look like this:

Risk level	**High Risk**	**Moderate Risk**	**Low Risk**
Description	Protection of the data is required by law/regulation, or The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our mission, safety, finances, or reputation.	The data is not generally available to the public, or The loss of confidentiality, integrity, or availability of the data or system could have a mildly adverse impact on our mission, safety, finances, or reputation.	The data is intended for public disclosure, or The loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on our mission, safety, finances, or reputation.
Data Example	Credit/Debit Card Number Tax File Number	First name, Last name and email combination Dietary requirements Membership numbers Student Ids May include: Any custom data customer need to use for communications purposes	Information in the public domain
Storage and Transmission	Storage of high risk data is prohibited	Encryption in transit is required.	Encryption in transit is required.

		Encryption at rest is required.	Encryption at rest is required.

Conclusion of Client Engagement

When business relationships end, Swift Digital follows specified and documented procedures for returning client data to the owner and permanently deleting it from our systems. We handle those tasks immediately upon satisfaction of all contractual requirements including financial settlements to the satisfaction of both parties, or in accordance with other stipulations.

Material in Question

Data to be returned includes all original information provided to us at the beginning and at any time during the engagement, as well as all data and work product brought into the systems by any means and for any purpose during the engagement.

Method of Return

Data can be returned by Swift Digital on storage media as agreed by both parties, or extracted from our servers. Successful removal and return of client data will be documented and confirmed in writing by both parties.

Permanent Deletion

Once client data is returned, Swift Digital will physically and/or electronically destroy all original data and work product. This includes all backups and reproductions of any kind. Data destruction will be permanent. Any physical devices, such as servers and other storage media that may retain any recoverable client data will be physically destroyed.

User Controls and Authentication

Each customer's privileged information is secured against unauthorized access by: (a) Non-compliant client users, (b) Swift Digital personnel and (c) Third parties such as vendors and hackers.

User Roles and Access

Swift Digital Suite has two user roles:

- **Administrator** is the highest-level role. Administrators can access all features in the suite and all records that have public or limited access. Only private data owned by other users is inaccessible to the administrator. The administrator is the only role allowed to add, delete and limit access of standard users.
- **Standard Users** are personnel authorized to perform general or specific tasks as determined by the administrator.

Customer Account Security

Swift provides a multi-tenanted cloud-based solution. Data is segmented in the database by Account ID, and client information is not accessible from one instance to another. As a SaaS model, support components are shared, but customer data is strictly segregated.

'Silo-ed' data ensures that customer data is account- specific and cannot be accessed from another account.

Your data is exclusively for your own purposes. Swift Digital does not share, sell or expose data to third parties.

Users can choose to allow or deny search engine indexing on an account-by-account basis. A function to whitelist / blacklist IP addresses is available on an account-by- account basis.

Valid logins and use of privileged data by client users are secured at four points: Usernames, Passwords, Session Tokens and SSL. Users are required to register with their name, phone number, email address and unique password. Login passwords must have 8 characters, with a combination of letters and numbers and the account is auto locked after 8 failed login attempts. All stored login credentials are encrypted. Whenever a live browser closes, the session expires and the user is logged out automatically.

Data Breach and Notifications.

Swift monitors all systems via live monitoring via Brocade, Splunk and New Relic, augmented by daily human reviews of our firewall and server log files for any suspicious activity.

Should a security breach occur affected customers would be notified by email and phone.

Swift Digital Employees

Swift Digital personnel only have access to information about our clients and to client resources and data as:

1. Mutually agreed upon in contracts, disclosures and other written documentation,
2. Requested by the client to maintain, repair or provide other professional services.

Because potential intruders actively seek new areas of both human and technical vulnerability, Swift Digital limits employee access to servers. We have tiered employee clearance levels and all activity is recorded.

All employees are trained to know and identify security threats, and to understand the risks and penalties they face by violating security rules or aiding those who do.

All staff undergo mandatory police background checks.

Third Party Access

Swift Digital prohibits and guards against all third-party access unless detailed in written agreements or other documents. If and when client administrators grant third- party access to the Swift Digital Suite and its data, the client is responsible for unwanted results or damages.

Summary

Swift Digital Suite and other cloud computing tools have improved how business people communicate with their teams and customers. These centralized functions enable companies of all sizes to compete far more creatively, effectively and affordably than would have been possible a few years ago.

At the same time, the complexity of data and Internet technologies offers virtually limitless opportunities for intellectual property to be compromised. Related risks and threats can never be taken lightly. Cloud computing services must rely on both technical and human processes to defend against threats.

Therefore, Swift Digital's security program combines the strength of the world's most credible data center, the proven efficacy of superior software and a wary and watchful security team to protect our clients' vital information at all times.