
# DG Enterprise Security

Version 2.4

digitalglue.com.au
Johnsons Building, Level 5 36 Grosvenor St, Sydney NSW 2000
p: +61 1300 787 615  f: +61 2 9475 5441

# Contents

# Document Control

## Release and Copyright Notices

| | |
|---|---|
| **Distribution control** | This document is subject to distribution control |
| **Property of Digital Glue** | This document is the property of the Digital Glue and is commercial in confidence. It is only authorised for distribution to approved Stakeholders of the Project and may not be otherwise shared without the express written permission of Digital Glue. |
| **Document Manager** | The person responsible for initiating, managing reviews and publishing final version/s of this document is: **Mahdi Zargar** |
| **Application of Change** | Anyone reviewing this document should mark their edits using the 'Track Changes' functionality and return their version to the Document Manager for incorporation into the next version Release. |

## Amendment History

| Version | Date Created | Created/ Amended By | Change Detail |
|---|---|---|---|
| **0.1** | 06/10/14 | Bouny Mounarath | Initial version |
| **0.2** | 08/10/14 | Charlotte Middleton | Updated based on Initial Review comments |
| **0.3** | 10/10/15 | Mahdi Zargar | Updated based on 2nd Review Comments |
| **1.0** | 13/10/15 | Bouny Mounarath | Signed Off V1.0 |
| **1.1** | 10/11/15 | Chris Tasker | Updated to agreed DG document format |
| **2.0** | 15/02/16 | Mahdi Zargar | Updated - PCI DSS Docs Added |
| **2.4** | 01/03/17 | Mahdi Zargar | Minor Changes |

## Distribution

| Recipient | Role/Team Company |
|---|---|
| Anthony McNamara | Managing Director – Digital Glue |
| Peter Malycon | Commercial Director – Digital Glue |
| Charlotte Middleton | Executive Producer – Digital Glue |
| Bouny Mounarath | Head of Development – Digital Glue |

# Introduction

## Purpose

The purpose of this document is to clearly outline the enterprise security policy that Digital Glue employs. Contained within are the details of the security framework and how it is applied throughout Digital Glue as well as the details of the data security layer in place. The policies contained within provide the basis for the security of each of Digital Glue's programs and infrastructure.

## Background

Digital Glue as a provider of software solutions have a responsibility to their clients to ensure that rigorous safeguards are in place to protect client and user information. These policies adhere to current best practice and have been developed specific to Digital Glue

## Objectives

The objective of this document is to outline the policies in place as well as any standards or guidelines applied by Digital Glue in relation to Enterprise Security. This document will form the base of all security procedures within Digital Glue's applications and inform the design of new programs.

## Scope

This policy applies to all information resources, systems or facilities (existing or new) where access controls are assessed to be required.

This document will outline the policies and procedures for:

- Enterprise security Framework
- Digital Security Layer
- Application & Database Security & Life-Cycle management
- Information Security & Life-Cycle management
- Information Security
- Infrastructure Architecture & Security.

The design details and security features of individual programs and applications is considered out of scope for this document.

## Related Documents

| Document Name |
| --- |
| DG_ Key Management Policy |
| DG_Acceptable Encryption Policy |
| DG_Access Management Policies and Procedures |
| DG_Account Creation and Termination Procedures |
| DG_Anti-Virus Policy |
| DG_Audit Policy |
| DG_Backup Policies and Procedures |
| DG_Change Management Process |
| DG_Incident Management Process |
| DG_Information Sensitivity Policy |
| DG_Password Policy |
| DG_Privacy Policy Information and Procedures |
| DG_Remote Access Policy |
| DG_Secure Data Destruction Policy |
| DG_Security Policy |
| DG_Server Security Policy |
| DG_Virtual Private Network Policy |
| DG_Vulnerability Assessment Policy |
| DG_Wireless Communication Policy |

# Digital Glue Enterprise Security Framework

Digital Glue (DG) Enterprise Security Framework (ESF) subscribes to the ISO 27001 Information Security Management System ISMS. DG's hosted facilities are contained within Amazon Web Services (AWS) infrastructure – AWS is ISO 27001:2005 certified[1].

DG's ESF implements the philosophy of ISO27001 industry standards regarding the security of applications, hosting environments and data protection. The ESF is a composite framework from the following:

***Digital Glue Enterprise Security Framework***

- Security Governance Framework
- Information Security Policy
- Access review, validation and remediation
- Asset management
- Information handling controls
- Security incident and breach notification process

***DG ESF Divisional Responsibilities***

- Application Life-cycle - DG
- Data Management - DG
- Infrastructure – AWS (Amazon Web Services)

# Data Security Layer

| Area | Description |
|---|---|
| Data Access | User access to raw or computed big data has about the same level of technical requirements as non-big data implementations. The data should be available only to those who have a legitimate business need for examining or interacting with it. Most core data storage platforms have rigorous security schemes and are augmented with a federated identity capability, providing appropriate access across the many layers of the architecture. |
| Application access | Application access to data is also relatively straightforward from a technical perspective. Most application programming interfaces (APIs) offer protection from unauthorized usage or access |
| Data encryption | Data encryption is the most challenging aspect of security in a big data environment. In traditional environments, encrypting and decrypting data really stresses the systems' resources. This problem is exacerbated with big data. The simplest approach is to provide more and faster computational capability. A more temperate approach is to identify the data elements requiring this level of security and encrypt only the necessary items. |
| Threat detection | The inclusion of mobile devices and social networks exponentially increases both the amount of data and the opportunities for security threats. It is therefore important that organizations take a multi-perimeter approach to security. |

[1] AWS Receives ISO 27001 Certification:
http://aws.amazon.com/blogs/aws/aws-receives-iso-27001-certification

# Application & Database Security & Life-Cycle Management

Application security refers to the measures and controls taken throughout the application lifecycle and the security measures employed to protect illicit access, data exposure and upgrade or maintenance of the application.

| AREA | DESCRIPTION |
|---|---|
| Authentication / Authorisation | Access to all administration web portals requires username and password credentials. Passwords are encrypted; password length and character set are enforced. |
| Change Management Processes | DG follows a set change management process: Identify change with customer – assess impact of change – develop roll-back plan – schedule update at time with minimal impact on production system – release, test, confirm to stakeholders. |
| Database Connection | Application database connection strings are encrypted with 256-bit RSA encryption algorithm. |
| Encryption (Symmetric and Asymmetric) | Bank data encryption – uses 256-bit key RSA encryption algorithm. |
| n-tiered Layer Architecture | Applications are designed and architecture in n-tier model, whereby the UI application (web portal) module is separated from the application server and a 3rd separation to the Data Store. This not only has a logical separation but physical separation. Generally, the Web Port will be exposed publically on the internet (DMZ) and then the application server component and database server are managed within a fully locked down private secured network with firewalls for traffic controls. |
| PCI-DSS | DG does not require PCI accreditation, as we do not store credit card information within our applications. If required, DG would implement such requirement where applicable. |
| Sensitive Details | Encryption of sensitive data – this is optional and assessed on a per application basis. DG web applications are publicly available via the internet - to protect sensitive data between client and server SSL connections enforced. |
| SSL- encrypting data over internet | All application/web portals requiring transport data protection over the internet use industry-standard 256-bit encryption.<br>SSL (Secure Socket Layer) security guarantees data being sent from the browser/client application to the application server is securely encrypted from prying eyes. |
| Audit | DG uses Database Server Audit log feature whereby DB administrator can centrally manage and regularly monitor potential unsolicited database activities. |
| Uptime | At least 99.95% uptime SLA[2] across AWS hosting infrastructure per month and 99.50% per month uptime for hosted applications. |
| Back-up strategy | Data in general is unencrypted and stored on database servers. Passwords and credentials are encrypted for local storage. Application and source code is backed up off site.<br>DG makes automat snapshot of the servers frequently based on the SLA. |

[2] AWS Security Centre:
http://aws.amazon.com/security/

| | |
|---|---|
| | DG creates daily ***encrypted*** (AES 256) differentiate SQL backup and weekly full SQL backups in Amazon S3 storage which is the most reliable storage that has replication across different regions.<br>DG exclusively uses the Asia Pacific (Sydney) region for Application and Database servers, data backups for DR are also stored within this region. But for complete redundancy, DG will use other AWS region as a secondary DR storage to mitigate any major catastrophe event to the AWS Asia Pacific (Sydney) region. Should a client's policy prevent DG from storing their redundant backups in an AWS region outside Australia, DG will source alternate storage location within a secured Australian premise. |
| Database access and protection | Production database is housed at a secured zone in AWS, only secured personnel who have been subjected to police and security background checks with administrator rights can gain access. Database backups are encrypted mitigating the data exposure in the event that the backup file falls into unauthorised hands. |
| Data isolation | All data is stored in separate databases within a virtual environment and logically separated within our multi tenancy platform. |
| Encryption of data | It is DG's policy to encrypt sensitive data like bank details; encryption of such data is done at a data level. However, DG does not encrypt data at a database/table level as this will severely degrade applications performance and general database functionality will be lost. |
| Exporting data to third parties | No direct access to databases is provided to third parties. Third party's access and requirements are rigorously reviewed, monitored and subjected to confidentiality agreements. |

# Information Security

| AREA | DESCRIPTION |
|---|---|
| Data housed in portable devices | DG does not permit data to be stored in portable devices unless formally approved by the client. Access to customer data is limited via the CRM search criteria. Mass data extraction is not possible for unauthorised staff. Portable devices are not permitted by staff. Only authorised staff can access customer data if signed off and recorded within audit trail. |
| Handling customer information | Full administration user guides are provided to all stakeholders who interact with the system. On-site training can be provided from finance to customer service to development; each responsible staff member has on-boarding training procedures as well as scheduled training sessions on systems and security. User guides stipulate user access and functions as well as security processes. As part of final training processes, each staff member signs a security declaration before gaining access to any administration system. This is renewed each quarter. DG clients are also subject to security declaration sign-off before being granted any access. |
| Customer data protection | DG is responsible to protect and properly govern our clients' and their customers' data contained within our secured AWS infrastructure. DG adheres to all protective measures around customer data protection in accordance with the Australian Privacy Laws.<br>AWS has released a whitepaper detailing and addressing their compliance obligations and considerations in regards to the Australian Privacy Act. |

| | |
|---|---|
| Incident management | DG has not had an incident of security breach ‘ever’ due to the high levels of infrastructure within AWS. These processes are managed by internal regulations. |
| Independent assessments | DG has enlisted a certified independent systems provider to certify security and software for lottery and gaming engine certification. |
| Professional indemnity | DG has full professional indemnity insurance cover. |
| Staff privileged information and confidentiality | All staff sign confidentiality clauses in contracts. In addition, undergo continual training in regards to the treatment of ‘sensitive and confidential’ material. |
| Staff background checks | Background checks are performed at time of employment before any staff can engage or interact with sensitive areas of the business. |
| Electronic communication applications | Email / IM / VOIP / SMS: All is protected by firewalls and IP routing as well as SSL. |

# Infrastructure Architecture & Security

DG's managed infrastructure and hosting is housed within the AWS Data Centres in **Sydney**. The AWS cloud infrastructure has been architected to be one of the most flexible and secure cloud computing environments available today. It provides an extremely scalable, highly reliable platform that enables customers to deploy applications and data quickly and securely.

### World-Class Protection

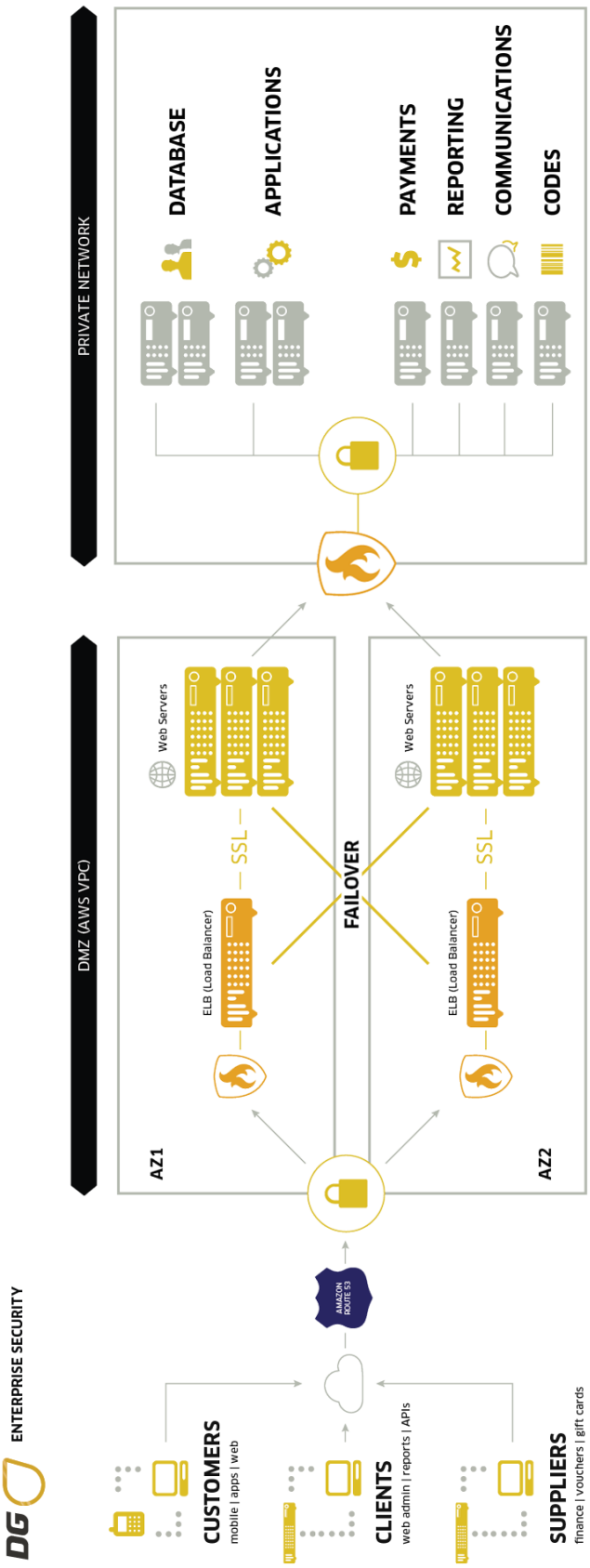
With the AWS cloud, not only are infrastructure headaches removed, but so are many of the security issues that come with them. AWS's world-class, highly secure data centres utilize state-of-the art electronic surveillance and multi-factor access control systems. Data centres are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis. Environmental systems are designed to minimize the impact of disruptions to operations. And multiple geographic regions and Availability Zones allow you to remain resilient in the face of most failure modes, including natural disasters or system failures.

### Built-in Security Features

Not only are applications and data protected by highly secure facilities and infrastructure, but they're also protected by extensive network and security monitoring systems. These systems provide basic but important security measures such as distributed denial of service (DDoS) protection and password brute-force detection on AWS Accounts.

| AREA | DESCRIPTION |
|---|---|
| System management | DG only uses certified hardware and software componentry. All upgraded components are approved by an information security resource. Monitoring is in place. DG has processes and procedures to manage data capture and change tracking. |
| Network configuration | The data centre environment is managed and controlled within Amazon's AWS infrastructure.<br><br>Networks and systems are closely monitored 24/7 by AWS CloudWatch and Nagios monitoring system. Access and permission levels to create or modify user rights; and / or change network / systems architecture is limited to only System Administrators. |
| Server redundancy | All servers within AWS infrastructure have been provisioned with redundancy and failover.<br>DG provides different level of high availability and redundancy for clients based on the SLA (Cold Disaster Recovery [DR], Warm DR, Hot DR and Multi-Cloud High Availability). |
| Self-defending firewalls | There are multiple levels of security within the network structure.<br>Checkpoint firewall with intrusion detection (IDS) and prevention system in the first level then VPC Security Groups and Network ACLs in the second layer and at last machines' firewall (Windows Firewall, Linux IPtable).<br>Traffic trying to request web portals is subject to security firewall policy checks.<br>Firewall policies can automatically enforce traffic block from unknown source of requesters.<br>VPNs and IP permissioned firewalls are used for internal networks as well as access to all System Admin functions. |
| Business Continuity Plan | BCP in place: In the event of adverse catastrophic event that may cripple the Sydney's Amazon AWS data centre, DG's BCP implements a redundant and failover to another Amazon AWS data region. |

| | |
|---|---|
| Malware protection | Malware / antivirus protection for PC's / laptops within the company network, malicious databases are updated every 24hrs and scanned every 24hrs. Servers and network environment are secured via Linux and Windows Firewalls. |
| Web server and SSL certificates | All DG administration sites are protected with SSL - this guarantees that data to and from the browser to the web server travels through a security connection whereby data is uniquely encrypted. |
| **SYSTEM DEPLOYMENT** | |
| Deployment procedures | Deployment of application to staging environment. Testing of application functions, security and information integrity / database connections.<br>Deployment to live environment testing, installation of SSL connections and lock down of production environment via firewall. |
| Change management processes | DG follows a set change management process: Identify change with customer – assess impact of change – develop roll-back plan – schedule update at time with minimal impact on production system – release, test, confirm to stakeholders. |
| Application isolation | Application server and database server at customer's demand can be set up to run on dedicated server separate from other tenants. This level of isolation will guarantee that other tenant's applications do not potentially gain other tenant data by mistake. |
| File transfer | File transfer or information movements between applications or customers using Secure File Transfer Protocol. |
| Access management | DG server administration is performed by the System Administration Team.<br>All maintenance activities are logged. Identity and access management procedures permit different server access to different levels of users with strong passwords with 90 day reset, activity logs and procedures reviewed quarterly.<br>No direct access is provided outside the System Admin team. |
| **PERSONNEL ACTIVITES** | |
| Staff privileged information and confidentiality | All staff are subject to confidentiality clauses in contracts. Training on dealing with privileged and confidential information on commencement as well as periodically. |
| Staff background checks | All personnel that have access to sensitive material are subjected to clearance checks. |
| **AUDIT AND REVIEW** | |
| Penetration testing | Third parties are engaged to perform tests on a periodic basis. Clients are also encouraged to undertake this as part of the on-boarding procedure. |
| Audit | DG uses Database Server Audit Log feature; whereby DB administrator can centrally manage and regularly monitor potential unsolicited database activities. |
| Independent assessments | DG has enlisted a certified independent systems provider to certify security and software for lottery and gaming engine certification. |


ENTERPRISE SECURITY
CUSTOMERS
mobile | apps | web
CLIENTS
web admin | reports | APIs
SUPPLIERS
finance | vouchers | gift cards
AMAZON ROUTE 53
DMZ (AWS VPC)
PRIVATE NETWORK
AZ1
AZ2
Web Servers
Web Servers
SSL
SSL
ELB (Load Balancer)
ELB (Load Balancer)
FAILOVER
DATABASE
APPLICATIONS
PAYMENTS
REPORTING
COMMUNICATIONS
CODES