TORQUE SOFTWARE

FMCS SECURE HOSTING GUIDE

July 2018

CONTENTS

INTRODUCTION

The Financial Management and Compliance System (FMCS) is a web based application used by Government agencies to manage financial governance and other administrative requirements. The FMCS is available under a Software as a Service (SaaS) arrangement. This document contains information about the hosting services provided when using FMCS under SaaS.

HOSTING SERVICES

Corporate Secure Hosting

Hosting Partner

Torque Software's partner for Corporate Secure Hosting of the FMCS is Amazon Web Services EC2 Cloud. Amazon has an outstanding reputation for delivering high quality and cost-effective hosting services, and runs some of the largest and most security-conscious sites on the internet.

For more information on Amazon's EC2 Cloud, visit https://aws.amazon.com/ec2/

ASD Certified Cloud Service

Amazon Web Services are certified for use for Unclassified workloads as per the Australian Government security classification system. Amazon Web Services meets the requirements of the Australian Government's **Information Security Manual** and **Protective Security Policy Framework**.

Supporting documentation is available as follows;

Amazon Web Services ASD Certification Statement of Compliance

Amazon Web Services IRAP Letter of Compliance

ASD Certified Cloud Services

Hosting Location

Servers are physically located at Amazon's EC2 Cloud in Sydney.

Physical Security

Amazon'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. Multiple Availability Zones allow resilience in the face of most failure modes, including natural disasters or system failures.

The AWS virtual infrastructure has been designed to provide optimum availability while ensuring complete customer privacy and segregation.

Risk and Compliance

Amazon is ISO27001 certified, amongst various other certifications.

Please see Amazon Risk and Compliance whitepaper here: http://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf

Connectivity

All Torque Software managed hosting options utilise multiple redundant high-speed internet links to provide more than adequate band width to deliver acceptable response times.

FMCS instance access can be configured to only allow connection from specific IP addresses, if required.

Gateway

Each Amazon VPC is a distinct, isolated network within the cloud; network traffic within each Amazon VPC is isolated from all other Amazon VPCs. At creation time, an IP address range is selected for each Amazon VPC. An Internet gateway, virtual private gateway, or both may be created and attached to establish external connectivity, subject to the appropriate controls.

Secure communication between client and server is ensured via TLS certificates.

Identity and Access Management

Identity and access management (IAM) is managed through Amazon's AWS IAM. See http://aws.amazon.com/documentation/iam/ for more information.

Application Migration

The FMCS can be migrated to local hosting services or another hosting provider at any time. If this is required, Torque Software will provide a backup of the FMCS

database and a copy of the application files, along with detailed instructions, for installation into the new hosting platform.

Technical support for hosting migrations is also available at additional cost.

Security Monitoring

Torque Software maintains and monitors the following logs, according to Microsoft and industry best practice, to detect any security incidents and ensure data security.

- AWS Cloud Trail. See http://aws.amazon.com/cloudtrail/ for more details
- Audit success and failure events in the system event category.
- Audit success events in the policy change event category.
- Audit success events in the account management event category.
- Audit success events in the logon event category.
- Audit success events in the account logon event category.

Clients are advised of any security incidents.

Windows Security

Firewall: All ports are closed by default with only ports 80, 443 and RDP open.

Port 80 is open only to redirect any unsecured clients to the secure instance on port 443.

RDP is locked down to only allow access from the static IP addresses of Torque Software for administrative purposes.

File system encryption is not required as the file system only contains compiled code.

Access control: All non-critical accounts disabled; administrative account is in non-standard name.

Virus/malware scanning: systems are locked down, disallowing new (unknown) processes to run.

System patching/updates: all servers are patched to the latest available versions of all software, as soon as those updates are released.

Security Clearances

All Torque Software personnel with access to hosted client environments have Australian Government Baseline security clearance and are vetted by personal interview and extensive reference checks.

Data Management Plan

Data Separation

Each client instance of the FMCS utilises a separate SQL Server database. Each client instance also uses a separate user account to connect to each client's database instance. This provides multiple boundaries between client data and ensures complete data separation.

Data Ownership

Ownership of the data is retained by the client. Torque Software will supply the FMCS data on request.

Backup Process & Schedule

The FMCS back up process is performed as follows:

- Database is backed up to disk at 11:00PM AEST
- Snapshot of entire virtual server (application files, database files and backed up database) is taken daily at 2:00AM AEST and stored on-site in redundant cloud storage at host
- Off-site backups are stored for disaster recovery purposes.
- Backups are taken and kept daily, and also on the first of each month, allowing roll-back to the start of the month or the previous day as appropriate.

Backup can be extended as required by the client at additional cost.

Recovery Process

When a database restore is required (database crash or similar), the last backed up database is restored from disk, meaning that maximum data loss is a single business day.

When a server restore is required, a new virtual server is created from the last snapshot and brought online. Application and databases are already configured under this approach, however if a new server is required databases can be restored from disk and the application can be redeployed by Torque Software.

Timeframe for the recovery process is within one business day.

Disaster Recovery Plan

When a prolonged outage or catastrophic host outage occurs and snapshots are inaccessible, new servers are provisioned from another provider and brought online rapidly using the off-site backup.

Torque Software maintains arrangements with Macquarie Telecom's Intellicentre (see http://www.macquarietelecom.com/why-mt/data-centres/intellicentre-2-macquarie-park/ for more details) as an alternate hosting provider to simplify and assure migration in case of a significant DR/BCP event.

Timeframe for disaster recovery is within three days.

Decommissioning and Data Sanitisation

Data sanitisation is performed using the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data whenever magnetic storage is decommissioned.

Incident Response Plan

An incident is any event that impacts the confidentiality, integrity or availability of the FMCS application or database. This includes, but is not limited to the following:

- Attempts to gain unauthorised access to FMCS or its data, except for unsuccessful logon attempts that are not repetitive in nature
- Disruption or denial of service, other than scheduled outages
- Loss of information confidentiality
- Loss of information integrity
- Infection of the FMCS by unauthorised or hostile software
- Theft or damage of physical assets used by the FMCS
- Unusual system behaviour
- Unauthorised use of the FMCS for processing or storage of data
- Changes to system hardware, firmware or software without the knowledge of Torque Software and/or the client

Security incidents are investigated by Torque Software's Senior Technical Advisor. Should an incident be identified, the evidence of the incident shall be preserved by taking a snapshot backup of the complete server. This includes the FMCS

application software, database, security monitoring logs and Amazon logs. The backup will be made available to the client for investigation if required.

Torque Software will formally report any incidents that effect, or could potentially affect clients, to the nominated contact of the hosted client by email. Torque Software will also attempt to contact the nominated client contact by phone. This advice will be provided as soon as practicable.

If the incident requires immediate withdrawal of service to mitigate any system damage or security risk caused by the incident, this may be performed without client consultation.

Any further action required to mitigate or repair any damage caused by the incident will be performed in consultation with the client. Actions taken may include any or all of the following:

- Database recovery
- Application re-install
- Additional security measures

Upon completion of any mitigation or repair actions, Torque Software will supply a detailed report to the client of the incident, including all actions taken.

Hosting Benefits

Hosting using Torque Software's services, compared to hosting on a client's own intranet, has the following benefits:

1. Immediate access to system upgrades as soon as they are available. No delays caused by internal upgrade schedules.
2. Should additional resources such as data storage capacity or CPU be required due to increased usage, this can be arranged very quickly.
3. Client's internal environment is simplified and support requirements and associated costs reduced.
4. Clients who have users that do not have access to the client's intranet may all access the same FMCS application.

HOSTING SERVICES OPTIONS

The following options are available. Note: Some options incur additional fees.

Single Sign-On

Single sign on is also optionally available. Single sign on allows FMCS users to use their own network authentication to gain access to the FMCS. Using Single sign on means users do not need to enter a separate logon id and password to access the FMCS.

Torque Software provides two options for Single Sign On.

Option 1 – Torque Software's Propriety Single Sign On

This option is provided by Torque Software and is implemented as follows:

1. Torque Software provide the client with a small .NET authenticator application (or source code if building in SharePoint or similar is preferred) which runs on an internal IIS server or SharePoint server. Note: the server must be on the client's Active Directory domain so the application can transparently identify the user.
2. The authenticator application obtains the user's DOMAIN\LOGIN from active directory and generates a secure token with this, the current time and a client-specific FMCS instance code (provided by Torque Software).

Note: The FMCS SSO tool does not gather or use any information from the local domain other than the user's login and, if required for multi-domain clients, domain name.

3. Once the security token has been calculated, the authenticator redirects to the FMCS instance on Torque Software hosted servers using the secure token to authenticate the user.
4. The FMCS ensures the user and all other aspects are valid and allows login seamlessly.

When users access the FMCS URL, single sign on works as follows:

1. Users access the FMCS URL, usually as a link on the client's intranet.
2. If the user is not already authenticated in the FMCS (i.e. their session has timed out or they have never signed in), they are automatically redirected to the client's internal intranet URL housing the authenticator application. Note that because the authenticator application is hosted on the intranet

any external attempt to access the FMCS will redirect to a non-existent URL.

3. The authenticator application performs the authentication and redirects the user back to the hosted FMCS.
4. This results in a seamless, transparent login experience so they never see a login screen.

The benefit of this approach is once the authenticator application is on the client intranet there is no more configuration required.

Option 2 –VANguard Federated Authentication Service

VANguard is provided by the Department of Industry and Science and is recommended for Federal Government agencies wishing to obtain authentication services for internet applications.

The VANguard Federated Authentication Service allows users logged on to their own Federal Government agency's network to authenticate and then use web applications such as the Financial Management Compliance System. Authentication occurs transparently without additional credentials or software being required on the user's computer.

Please see this page for more information about VANguard.

To check if your department is already using the VANguard service, please see this page or contact VANguard.

Defence Signals Directorate Certified Gateway Hosting Option

Optionally, hosting services can be provided using a Defence Signals Directorate certified Gateway. Note: additional fees apply for this option. Typical fees are significantly more than the Corporate Secure Hosting described above.

Hosting Partner

Torque Software's partner for hosting the FMCS with a Defence Signals Directorate Gateway is Macquarie Telecom's Intellicentre. For more information on Macquarie Telecom's data centres, visit

http://www.macquarietelecom.com/why-mt/data-centres/intellicentre-2-macquarie-park/

http://www.macquarietelecom.com/why-mt/data-centres/hosting-certifications-and-accreditations/

Hosting Location

Servers are physically located at Macquarie Telecom's Intellicentre in Sydney.

Physical Security

Macquarie Telecom's Intellicentre is engineered to the first-class standards required to support the highest level of accredited security & availability for mission critical application hosting, IT infrastructure and intellectual assets.

- Security certifications include: ISO27001, ASIO T4 Intruder Resistant and Defence Signals Directorate (DSD) "Highly Protected". It also has Payment Card Industry (PCI DSS) certification.
- Australian based: All data resides completely within Australia.
- Enterprise-grade hardware: suppliers include EMC, Juniper, Hewlett-Packard and Dell.
- Multiple physical security measures protecting access: including mantraps, access-cards, biometric scanning and round-the-clock interior and exterior surveillance monitors.
- CCTV: including motion detection and fixed cameras with digital recording and archiving.
- Background security checks: all employees undergo multiple security checks. Access to the data centre is limited to those with legitimate business needs.

Additional Hosting Options

The following optional services are also available.

- Full database encryption using Transparent Data Encryption (TDE). Note; this may have some impact on response time or increased hosting fees for the additional server resources required to balance the encryption overhead.
- Database recovery using transaction logs to roll forward to a particular time of day
- Access to audit logs
- Assistance with security investigation or legal discovery

PRIVACY

Torque Software adheres to the Australian Privacy Principles contained in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* for all personal information held within the FMCS.

All reasonable steps are taken to protect personal information from misuse, interference and loss, and from unauthorised access, modification, or disclosure. Personal information collected by the FMCS includes names and email addresses. This information is collected as part of the normal user registration process or as provided and uploaded by authorised FMCS administrators. Personal information is held within the FMCS database. The only purpose for collecting personal information is for the purpose of using the FMCS. Individuals may access their own personal information by using the My Details option within the FMCS. Individuals who believe a breach of the Australian Privacy Principles has occurred may contact the FMCS system administrator or Torque Software to register a complaint.

No personal information is disclosed to overseas recipients. In any other circumstance personal information is only provided to other persons where it is required as part of the normal operations of the FMCS.

To learn more about Torque Software, contact us on 1300 795 581 or visit www.torquesoftware.com.au.

TORQUE SOFTWARE