*Updated: November 2015*

# TECHNOLOGY ARCHITECTURE

## HIGH-LEVEL SUMMARY

Abintegro provides cloud-based (SaaS) careers technology. The system includes a variety of web-based resources and applications focusing on career management and career transition. Our UK technology hosting partner is Memset Limited.

The two main logical components of our system include an administrative portal (Career Centre Manager - CCM) and a client portal (Career Centre - CC). Both portals are accessible only through an authentication process.

CC - Communication between the client browser and the application servers use both HTTP and HTTPS protocols. HTTPS (secure) protocol is used where client data is exchanged.

CCM - All communication between the client browser and the application servers use the HTTPS protocol.

User connects using a standard web browser (Internet Explorer, Chrome, Firefox, etc.). No additional software or plug-ins are needed.

Abintegro support a number of proprietary Single Sign On solutions in addition to industry standards including, ADFS, the UK Access Management Federation (www.ukfederation.org.uk) where we are a Shibboleth 2 Service Provider.

All usernames and passwords are stored in the client's specific database. Passwords are hashed together with a salt using HMACSHA1. In addition all query string URLs are encrypted where they contain user-specific information.

Browsers must allow for non-persistent cookies and be JavaScript-enabled. The majority of resources within both applications are also available on mobile tablets including iPads.

Abintegro provides on-going technical support as part of the license. Phone and email support is available during normal UK business hours. Urgent after-hours technical support is available if necessary.

System support, guides and documentation are also built into the application via help / training videos, written instructions within the application and an administrator knowledge base is also available in the CC and CCM administrative system.

The system benefits from the following security countermeasures:

- Data transmission encryption of all personal, sensitive, data

- Managed firewall (hardware and software) / Anti-virus software

- Monthly vulnerability scanning and testing, penetration testing and resolution

- User-managed data security through individually password protected accounts

- Data transmission security - TLS Certification provides data transmission encryption where supported by the user’s browser. Where TLS is not supported, connection will not be permitted.

- IIS8.5 lock plus Microsoft security policy and best practice server hardening (including, but not limited to, password policy and expiry, folder permissions, open ports)

*Updated: November 2015*

**FULL DETAILS**

## COMPANY AND PRODUCT INFORMATION

### 1) Company name and registered address.

Abintegro Limited - 19 Seer Mead, Seer Green, Beaconsfield, Bucks, HP9 2QL, UK

### 2) Company name and address of technology hosting partner.

Memset Limited - Building 87, Dunsfold Park, Stovolds Hill, Cranleigh, GU6 8TB, UK

### 3) Product description.

Abintegro provides cloud-based (SaaS) careers technology. The system includes a variety of web-based resources and applications focusing on career management and career transition.

## APPLICATION ARCHITECTURE

### 4) Overview description of the end-to-end application.

Clients login to the Career Centre (CC) application through web-based forms utilising secure HTTPS protocols (The connection is encrypted using AES_256_CBC with SHA1 for message authentication and RSA as the key exchange mechanism). Data within the Career Centre classified as "sensitive" is transmitted using this secure protocol. Administrators accessing Career Centre data are required to use 128-bit integer number used to identify resources.

Administrators access the Career Centre Manager (CCM) application through web-based forms utilising secure HTTPS protocols (The connection is encrypted using AES_256_CBC with SHA1 for message authentication and RSA as the key exchange mechanism). All data is transmitted using this secure protocol.

The data exchange between the CC and CCM is managed via the Abintegro Web Service (WS).

Abintegro runs and maintains a secure WCF (Windows Communication Foundation) Web Service to allow data transmission between Career Centre and Career Centre Manager and integration with external client systems. WCF internal (CC and CCM) functionality is locked to Abintegro applications only and cannot be accessed by client systems - requiring specific username / password authentication. Access from external client systems is restricted to certain functions and locked-down to the specific client data - also requiring specific username(s) / password(s) authentication. Custom client functions are agreed, written and tested on a project-basis with scope to extend the range of web service functions significantly to support client requirements and client systems/integrations.

All data transmission through the Web Service is encrypted with TLS (256-bit encryption).

### 5) Application logical components.

The two main logical components of our system include an administrative portal (Career Centre Manager - CCM) and a client portal (Career Centre - CC). Both portals are accessible only through an authentication process.

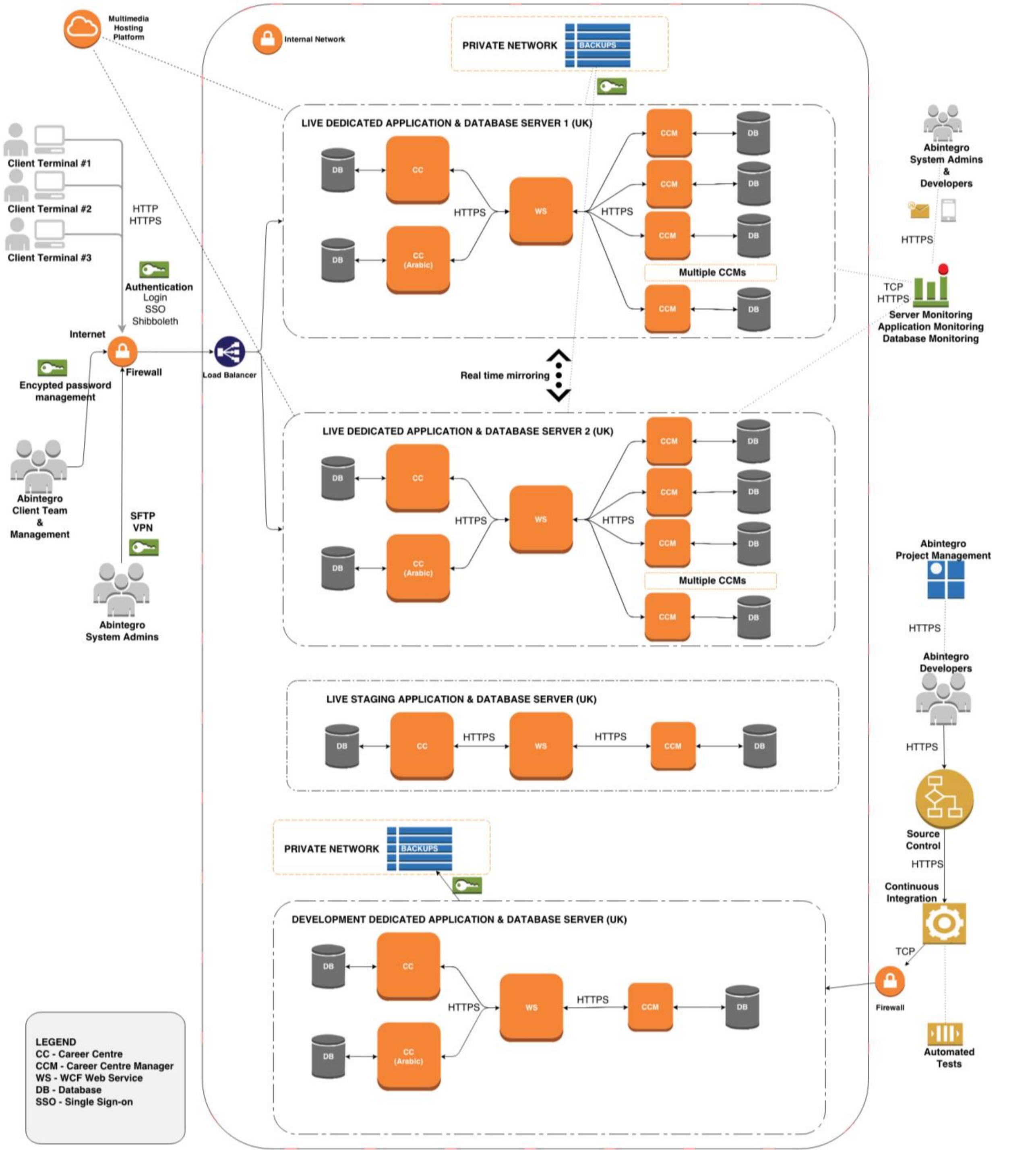
The CCM is utilised by designated "administrators" for each client, and contains the functionality to manage client data, run a variety of reports and configure application settings.

*Updated: November 2015*

The CC contains web-based tools and resources related to career transition and development, as well as custom content/e-learning modules.

Both logical components are housed on our dedicated servers within our server farm, separated virtually through each server's IIS service.

## 6) Application Architecture.



## 7) System Inventory (Technology Stack).

- Web Application: ASP.net C#

- Database: MS SQL server 2012

- Server OS: Windows 2012 R2 server, Internet Information Services (IIS 8.5)

- Sophos Antivirus

- Server monitoring service with auto-reboot

- Firewall (hardware and software): 24/7 managed firewall, DoS protection, Windows firewall

## 8) Protocols used to communicate between the application components.

CC - Communication between the client browser and the application servers use both HTTP and HTTPS protocols. HTTPS (secure) protocol is used where client data is exchanged.

CCM - All communication between the client browser and the application servers use the HTTPS protocol.

Communication between the CC and CCM is via web service (WCF) using HTTPS protocol.

Communication between the database and the application is performed using .NET SQLClient Connection objects utilizing SQL scripts.

All communication methods are industry standard.

## 9) Location, encryption of and access to configuration files.

Configuration files are located with the web application domain(s). Access to the production configuration files is limited to technical management and authorised developers.

Access is restricted to SFTP connections and IP restriction (via VPN access), both of which are protected by 1024 Bit SSH-2 RSA256-bit encryption keys.

## 10) Client/end-user registration process.

CC - End-user accounts are created through the following processes:

- Single/batch upload process by client administrators.

- End-user self registration (where permitted) via a secure sign-up page located with client's protected environment eg. Intranet.

- Single sign on / Web Service automated account creation integration with client systems.

## 11) Log-on function and authentication methodology.

End-users navigate or are directed to a secure login page where they are prompted to enter their username (email address) and password.  These fields are filled in and submitted through a secure connection (HTTPS) to the web application. The application server performs a variety of security checks, including checking the username login attempts. The username and password are compared against the production database to verify authenticity.

After the user’s status is verified, a .NET session is created and sent to the end-user in the form of a session cookie.

### 12) Data controls ensuring data is only accessible on a need-to-know basis and that a client/end-user can access only the data to which they are authorised.

Only those employees with the required skill and clearance are given access to sensitive systems and information. These systems are based on relevance to the employee's responsibilities and need to know and are reviewed periodically.

All CC client data is stored in a central CC database. Specific client data is separated by a unique client identifier. User data is bound to the client record and the web application only permits the individual user to access their own data. Each client organisation receives a unique identifier (Client Token) that is used to identify and segregate all CC activity data in the CC system. This identifier is used whenever retrieving end-user activity information or determining access rights.

Each client's CCM, holding end-user personal data, is specific to each client ie. separate, dedicated, database and CCM application. In addition encrypted query strings are used where applicable and data transmission encryption via TLS is utilised throughout.

### 13) Application integration with single sign-on security frameworks.

Abintegro support a number of proprietary SSO solutions in addition to industry standards including ADFS, the UK Access Management Federation (www.ukfederation.org.uk) where we are a Shibboleth 2 Service Provider.

### 14) Session management methodology.

Non-persistent cookies that contain encrypted ASP.NET session ID and in-memory session state objects are utilised.

### 15) Session management - ending a session / log off.

A "logout" button is available on both the CC and CCM that ends the session and removes the session cookie from the user's browser.

Session cookies are configured with an auto expiry of 60 minutes.

### 16) Storage of user IDs and passwords for validating user credentials.

All usernames and passwords are stored in the client's specific database. Passwords are hashed together with a salt using HMACSHA1. In addition all query string URLs are encrypted where they contain user-specific information.

### 17) Clients/end-users connection to the web application.

The user connects using a standard web browser (Internet Explorer, Chrome, Firefox, etc.). No additional software or plug-ins are needed.

The following web browsers are supported: Internet Explorer 9+, Google Chrome / Safari and FireFox (latest versions recommended). Internet Explorer 8 is no longer supported as Microsoft no longer provide security updates or technical support for Windows XP and, therefore, PCs running Windows XP / IE 8 cannot be considered to be protected from security vulnerabilities.

### 18) Method for addressing forgotten passwords.

The automated password reminder system allows the end-user to enter their email address, and if an account matches the supplied email address, a new (secure - 8 digit) password is generated and sent to that email address.

Passwords can also be reset manually by administrators within the CC and CCM.

### 19) Two-step authentication capabilities of the application.

Within the CC, administrators are required to enter their username and password to access the service and, subsequently, provide a 128-bit integer client token (Globally Unique Identifier - GUID) to activate all administrator functions.

### 20) Password security, expiry, forced change.

Passwords can be created in a number of ways:

- Single sign on process: passwords are system created and changed every time the user accesses the CC. A 10-digit, alphanumeric, password is auto created and managed by the CC application.

- Manual account creation by administrators: By default passwords are automatically created (see above using the 10-digit format). Passwords can be manually created by administrators - they must be at least 6 characters long and cannot match the user's first name, last name or email address.

The option is available to force CC passwords to be change upon first use. Administrator passwords are forced changed on a periodic basis.

### 21) Controls on repeated attempts to log on.

After five unsuccessful login attempts on the application, a user’s account will be locked for a period of five minutes.  The security team is notified once the account is locked.

### 22) Browser version requirements, compatibility, use of JavaScript.

The CC and CCM applications are available via all major internet browsers on both PC and MAC platforms including Internet Explorer v.8 and above, FireFox, Chrome and Safari. Where possible we always recommend using the latest version.

Browsers must allow for non-persistent cookies and be JavaScript-enabled.

The majority of resources within both applications are also available on mobile tablets including iPads.

No client-side components are needed.

| Requirement | Explanation |
|---|---|
| **Internet connection** | To access the Abintegro server. If you can freely view external websites (eg. Google.com) then you will be OK. Subject to internet browser restrictions, for example, blocking of certain file types/scripts by corporate firewalls. |
| **Internet Browser** | Abintegro supports the major internet browsers on both PC and MAC platforms including Internet Explorer v.8 and above, FireFox, Chrome and Safari. Where possible we always recommend using the latest version. |

| | |
|---|---|
| **Document export** | User documentation (CV downloads/exports etc.) are output to multiple file formats including: DOC, OOXML (XML), RTF, HTML, OpenDocument (XML), PDF, XPS (XML).<br>Other outputs / tutorials / guides are in .pdf format and require Adobe Acrobat reader which is freely available. |
| **Video & Audio tutorials** | PCs must have a soundcard and, if possible, support Adobe Flash to view/hear the videos. HTML 5 video fallback is also available.<br>The majority of Abintegro video and audio resources are also HTML 5 compatible and operate fully where Adobe flash is not installed eg. iPads, iPhones. |
| **JavaScript** | JavaScript needs to be enabled on the user PC. This is the default setting so ordinarily is only an issue if disabled by an IT department. |
| **Cookies** | Temporary session cookies are used within the login process to authenticate the user. User's internet browser must allow cookies. |
| **Operating system** | Major operating systems are supported, including Windows (XP, Vista, 7, 8), MAC OS X (all versions). |
| **PC/MAC compatibility** | Fully compatible on both PC and MAC platforms. |
| **Internet connection speed** | No minimum requirement, however, recommended above 1Mb/s. Videos are dynamically streamed with bit rate adjusted for connection speed. |

## 23) Types of reporting generated, storage and transport mechanisms.

Many standard reports are available to administrators in the CC and CCM. All reports generated in the system are transferred over a secure HTTPS channel, through a web browser interface. In some cases, .pdf, .xls or .doc versions are available, which are also transferred over a secure HTTPS channel. Reports are not saved in the system.

For specific client projects, reporting data is available via SFTP access. Data is also password protected and overwritten periodically.

## 24) System audit trails.

Application audit logs are generated for all client page requests, error messages, authentication operations, account creation, many administrative actions, system emails, and many critical database fields.

These are monitored constantly by the Technology Team. Any abnormal behavior is alerted and reviewed immediately. Although sensitive data is not stored in audit logs, it is given the same sense of security as any data being stored.

## 25) Use of open source code.

No open source code is utilised within our system.

## 26) Traffic distribution across servers (horizontal scalability).

Hardware load balancers distribute user traffic across the dedicated Abintegro servers. The load balancers are configured to maintain the user session/activity on the selected server throughout the duration of the active user session.

The application and database servers can be scaled in terms of number of servers as well as capacity and performance of each server.

The application tier is load balanced and currently contains 2 application servers. These servers can be individually taken offline to upgrade. Additional servers can be added to the farm.

### 27) Stress / load testing.

The system is tested using simulated load testing regularly as part of our software development cycle including the development of new applications.

These tests are performed at least annually, but typically are performed more regularly as deemed appropriate.

The application and system infrastructure is deliberately sized to cope with a user population of at least 10 times the normal operating population. As necessary, the system is scaled both horizontally and vertically.

### 28) On-going technical support.

Abintegro provides on-going technical support as part of the license. Phone and email support is available during normal UK business hours. Urgent after-hours technical support is available if necessary.

System support, guides and documentation are also built into the application via help / training videos, written instructions within the application and an administrator knowledge base is also available in the CC and CCM administrative system.

## ACCESS CONTROL AND APPLICATION ADMINISTRATION

### 29) Policies and procedures for password controls and session security.

Access to Abintegro assets including the Career Centre and Career Centre Manager is controlled by strict authentication mechanisms.  Access is granted based on the data classification of the resource and the need of the employee in their role to access the resource.  Password standards are set and enforced for the Abintegro network resources as well as the CC and CCM.  Session security is also managed in regard to time limits as well as to the type of data and encryption techniques utilised to secure that session.

### 30) Administrator application and data access.

The support team has the capabilities to login to the application as an Abintegro  Administrator, which allows access to mimic a client's login. This activity is specifically logged.

### 31) Remote access to the production servers including network connectivity.

Remote access to the Abintegro data centre is granted to authorised members of the Abintegro technical team and our managed hosting representative at Memset.

Access to the production servers is by SFTP, VPN and remote desktop, all of which requiring username/password, IP restriction and security key for SFTP connection. Memset access via their internal private network.

**Controls in place to protect production systems and data from unauthorised access.**

Direct access to the production systems and data is restricted to authorised personnel within the organisation. Access to Memset is made through a static IP/VPN connection.

There are no generic, temporary, guests, shared or group logins used.

## 32) Application access logs.

All user and administrator logins to the application are logged and stored in the database. These records are kept for 5 years before being removed. Access logs are reviewed by the Technology Team periodically.

## 33) Access controls to the system's production servers.

- Remote desktop (RDP): Access is restricted via static IP lockdown, only accessible via Abintegro secure VPN.

- VPN: Access to VPN from Client is encrypted (IPSEC). Accessed only by Head of IT and designated IT/Management staff.

- SFTP: Access to FTP is restricted to SFTP only (secure) with public key management.

- No other (excluding HTTP/HTTPS) access routes permitted to the system's server(s). Enforced via dedicated external firewall.

- Password policy includes password length, age (30 days maximum) and history check. User accounts are disabled after 5 unsuccessful logon attempts.

Access to local data is controlled as follows:

- Local Database/Application: All local databases only contain test user data.

- Password Management: All local passwords, authentication tokens and sensitive client system data stored in encrypted password management software.

## 34) Additional Security Countermeasures.

The system benefits from the following security countermeasures:

- Data transmission encryption of all personal, sensitive, data

- Managed firewall (hardware and software)

- Monthly vulnerability scanning and testing

- Penetration testing and resolution

- User-managed data security through individually password protected accounts. Passwords require a minimum of 6 characters and password strength indicators informs users of their chosen password strength.

- Data transmission security - TLS Certification provides data transmission encryption where supported by the user’s browser. Where TLS is not supported, connection will not be permitted. Our certificates are 256 bit and are trusted by over 99% of current internet users' web browsers.

- IIS8.5 lock

- Microsoft security policy and best practice Server hardening (including, but not limited to, password policy and expiry, folder permissions, open ports)

- Anti-virus software

- Unneeded network services are disabled, on the Windows Servers

**Detection, isolation and removal of malicious code**

The system is capable of the rapid detection, isolation and removal of malicious code by the following means: Anti-Virus software is installed on all system components as appropriate. The Virus definition files are updated on daily basis. Real-time scanning is running on all system components to ensure all files going to and from the system are scanned for the latest threats.

## DEVELOPMENT POLICIES AND PROCEDURES

### 35) Methodology for developing and testing infrastructure, systems and applications.

Abintegro follows the Microsoft Solutions Framework as a development methodology. This includes documented change control, development, testing, and deployment procedures including security testing.

### 36) Controls to prevent unauthorised changes to the application source.

All code is stored and tracked in TFS, which is managed by the Technology Manager. All changes to application code are stamped with each developer's name and a description of each change. Developers must be authenticated before making changes to source-controlled code. All versions are archived indefinitely, and code can be rolled back to any version.

### 37) Development and test environment segregation from the production environment.

The test / development servers are physically separate from the production servers.

The test / development servers do not contain any client or user data and operate with Abintegro test data only.

## SECURITY ORGANISATION AND POLICY

### 38) Information Security Organisation.

Abintegro has an Information Security Policy which has been in operation since 2010. Since then, policies have been updated from time to time as needed to keep up with legal, procedural and technological developments. They have been drawn up in line with the ISO/IEC 27001 standard.

Ultimate responsibility for information security rests with the Managing Director of Abintegro, but on a day-to-day basis the IT Director is responsible for managing and implementing related procedures.

Management are responsible for ensuring that permanent and temporary staff and contractors are aware of:

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

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

The information security procedures are maintained, reviewed and updated by the IT Director. This review takes place annually.

Management are individually responsible for the security of their physical environments where information is processed or stored.

Each member of staff is responsible for the operational security of the information systems they use.

Each system user is required to 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.

Abintegro is obliged to abide by all relevant UK legislation and the relevant legislation of the European Union. Of particular importance in this respect are the Computer Misuse Act 1990 and the Data Protection Act 1998. The requirement to comply with this legislation is devolved to employees and agents of Abintegro, who may be held personally accountable for any breaches of information security for which they may be held responsible.

Information security awareness training is included in the staff induction process.

Incident Reporting

All security incidents are the responsibility of the IT Director and remedial action is assigned by the IT Director to specified members of the Abintegro IT team.

Abintegro handle security incidents using the following 6-steps:

Preparation: IT staff education regarding the importance of updated security measures. Training to respond to computer and network security incidents quickly and correctly.

Identification: The response team is activated to decide whether a particular event is, in fact, a security incident.

Containment: The team determines how far the problem has spread and contains the problem by disconnecting all affected systems and devices to prevent further damage.

Eradication: The team investigates to discover the origin of the incident. The root cause of the problem and all traces of malicious code are removed.

Recovery: Data and software are restored from clean backup files, ensuring that no vulnerabilities remain. Systems are monitored for any sign of weakness or recurrence.

Lessons learned: The team analyses the incident and how it was handled, making recommendations for better future response and for preventing a recurrence.

## 39) External Security Review.

NCC Group (a global information assurance specialist) performed impartial, rigorous, Web Application / System Penetration Testing in May 2015 to highlight and categorise any security issues within the Abintegro systems. No high severity risks were identified. All medium risks were resolved. Low risk items are constantly reviewed by Abintegro and proactively addressed as part of our infrastructure security programme.

Additional information relating to the Abintegro data centre partner, Memset:

- UK-based, highly-resilient data centres, with tight physical and logical security suitable for private and public sector. CRB/Background-checked staff. ISO27001 certified.

- All support staff are CRB checked and cleared as well as BPSS cleared. In addition, the majority of support staff also have SC clearance - performed by CESG, allowing them to handle IL3 Data to "classifed" level for central/local Government clients.

Security Organisation and Leadership
MD oversight of security matters as Senior Information Risk Owner (SIRO)
Operational ownership of security matters held by a dedicated Security Manager
Segregation of duties between Security and Compliance managers and teams
Board representation in security decisions
Strong investment in security technologies, personnel and processes

Physical and Environmental Security
ISO 27001 certified data centres, Dunsfold datacentre accredited to IL3 and appropriate to IL4 for physical security
Comprehensive CCTV coverage with footage retained for 90 days
Biometric and/or RFID badge controlled access to data halls
Physical access limited to specific necessary personnel
Stand-off fenced perimeters in place
At least N+1 UPS, generators and HVAC
FM-200 fire suppression
Continuous Building Management System monitoring

Operational Security
Incident management and change control procedures in place
Active involvement in the security community
DevOps security model allowing rapid mitigation of security issues
Strict media sanitisation and destruction procedures
Role-based access control
Customer support activity logging

HR Security
All staff are BPSS screened prior to commencing employment
SC vetted staff
Defined and managed hiring and termination policies
Mandatory confidentiality agreements for all staff
Ongoing security awareness training for all staff

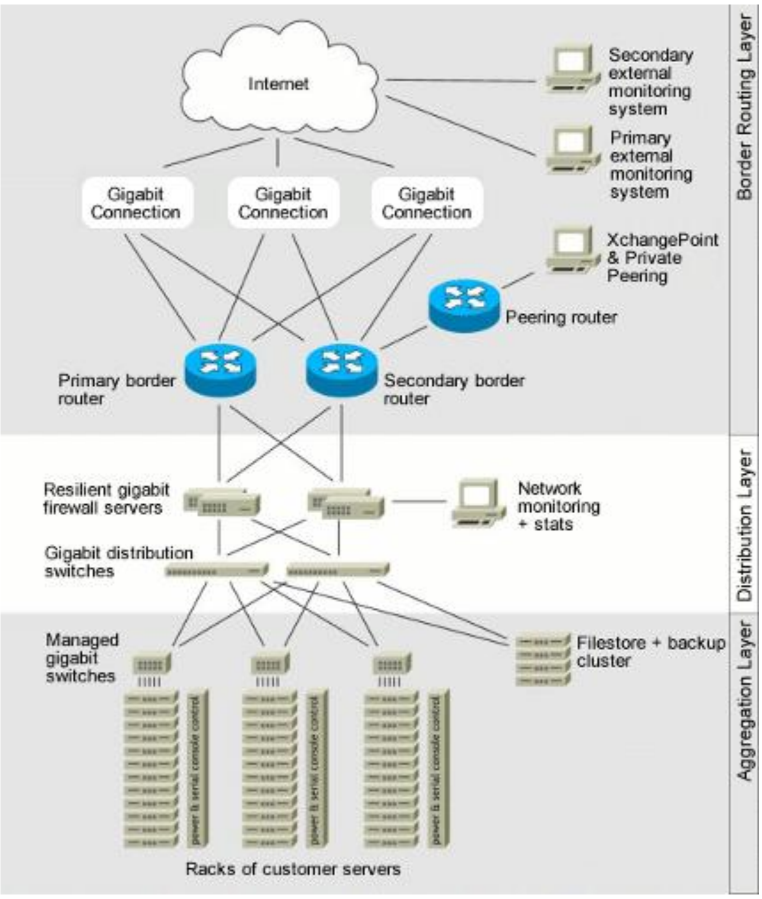
Compliance
ISO 27001:2013 certified hosting services and data centres
ISO 9001 and 14001 certified
PGA accredited to provide Official (IL2-IL3) services
Accredited to provide Official classified services via encrypted PSN overlay

More information can be found here:

Security, standards and accreditations: http://www.memset.com/about-us/security.php

ISO certification: http://www.memset.com/about-us/iso-certificates.php

Data centre: http://www.memset.com/about-us/datacentre.php


Internet
Secondary external monitoring system
Primary external monitoring system
Gigabit Connection
Gigabit Connection
Gigabit Connection
XchangePoint & Private Peering
Peering router
Primary border router
Secondary border router
Border Routing Layer
Resilient gigabit firewall servers
Network monitoring + stats
Gigabit distribution switches
Distribution Layer
Managed gigabit switches
Filestore + backup cluster
power & serial console control
power & serial console control
power & serial console control
Racks of customer servers
Aggregation Layer

Memset - Network Diagram

## DATA SECURITY

### 40) Data retention and secure disposal.

User data is retained for an agreed duration specific to each client project. After the agreed duration, data is automatically disposed for all client users and a data disposal confirmation is generated.

At any time client Administrators can archive User accounts. This immediately removes all personal information but does permit the account to be restored if required at a later date.

By default, all archived accounts and User accounts that have been expired for 6 months or more, are automatically disposed of (where the client has not already specified an agreed data retention period).

The system (application code and user data) is encrypted (AES encryption using industry standard component) and backed up automatically daily (to a secure network filestore) with a rolling 7-day storage. Backups are restored as necessary as part of the working practice of the technology team. In practice this means backups are restored at least once a month.

## PERSONNEL SECURITY

### 41) Pre-employment screening of employees.

All new employees undergo pre-employment screening for criminal background, employment and education verification, and reference checks.

In terms of general employee screening, below is a summary of the checks which Abintegro perform:

a) Where employees join via a recruitment agency, they provide Abintegro with employment reference checks.

b) For all employees, we run background checks utilising a LexisNexis KYC solution (online compliance, risk and fraud management solution), searching prospective employee names against 32,000 sources of news, company & financial databases included disqualified directors, sanctions lists, PEP lists and negative news checks. This service enables Abintegro to conduct consistent checks on individuals, directors and companies.

c) Abintegro run our own social media checks on employees (across main social platforms including: LinkedIn, Twitter and Facebook).

Abintegro do not use any sub-contacting staff for the provision of our services to our clients.

Additionally, all new employees undergo required security and privacy training as part of their induction programme.

### 42) Procedures for processing voluntary and involuntary employee terminations.

Upon voluntary or involuntary employee termination, all physical and logical access rights are revoked. Any hardware or data in the employee’s position is also retrieved. Confirmation of access revocation is conducted by the IT Director.

### 43) Employee information security responsibilities and confidentiality agreement.

All employees are required to sign a confidentiality agreement as well as undergo security and privacy training as a condition of employment. All employees are required to accept the company's computer usage policy. Memset provide HR security including ongoing security awareness training for all staff. Refer to: http://www.memset.com/about-us/security for further details.

## SECURITY PRACTICES

### 44) Firewall and intrusion detection.

Firewall (hardware and software): 24/7 managed firewall, DoS protection, Windows firewall.

24/7/365 firewall management is conducted by the managed hosting team at Memset.

### 45) Web sessions protection using TLS.

Web sessions are protected by utilising secure HTTPS protocols (The connection is encrypted using AES_128_CBC with SHA1 for message authentication and RSA as the key exchange mechanism). Data within the Career Centre classified as "sensitive" is transmitted using this secure protocol. Administrators accessing Career Centre data are required to use 128-bit integer number used to identify resources.

Administrators access the Career Centre Manager (CCM) application through web-based forms utilising secure HTTPS protocols (The connection is encrypted using AES_256_CBC with SHA1 [from March 2015 with the renewal of the certificate, SHA256 will be used] for message authentication and RSA as the key exchange mechanism). All data is transmitted using this secure protocol.

The data exchange between the CC and CCM is managed via the Abintegro Web Service (WS), all data transmission is encrypted with TLS (256-bit encryption) where supported by the user's browser. Where TLS is not supported, connection will not be permitted.

### 46) Web page protection against defacement by an intruder.

Defacement through server access is prevented by multi-tiered authentication utilizing a firewall, VPN connection and server administrative-level access. Defacement through scripting attacks is prevented by SQL Injection and Cross-Site Scripting prevention methods on all input fields.

### 47) Procedures to mitigate critical/high vulnerabilities including confirmation that systems are patched and up-to-date.

Abintegro utilise the latest version of Microsoft operating system and database technology (Windows 2012 R2 / SQL Server 2012). Any critical updates are deployed within 24 hours. All other non-critical updates are deployed within a 7-day deployment cycle. Antivirus definitions are automatically updated in line with the provider's recommended best practice. Windows server firewall is configured to only allow business critical network traffic.

Application vulnerabilities alerts are automatically monitored and patching is immediately applied and scheduled for emergency release.

### 48) Independent security reviews (audits), vulnerability scanning, and penetration testing.

Abintegro systems undergo monthly vulnerability scanning and testing. Security vulnerability scanning is the process of checking the servers regularly for possible routes of entry for a hacker or malcontent. We combine port scanning with regular vulnerability assessments of the servers configuration and software in order to highlight potential areas of exploit. We perform the scans from outside our / Memset's network in order to make it a "real life" test.

NCC Group (a global information assurance specialist) performed impartial, rigorous, Web Application / System Penetration Testing in May 2015 to highlight and categorise any security issues within the Abintegro systems. No high severity risks were identified. All medium risks were resolved. Low risk items are constantly reviewed by Abintegro and proactively addressed as part of our infrastructure security programme.

In addition software on our servers monitors changes to configuration and binaries, as well as providing a comprehensive audit trail of changes. Alerts are sent to Abintegro technical team whenever a significant event occurs on the servers allowing us to react where necessary.

The service is configured to level (10) - Defined as: multiple user generated errors - They include multiple bad passwords, multiple failed logins, etc. They may indicate an attack or may just be that a user just forgot his credentials.

## OPERATIONAL PRACTICES AND PROCEDURES

### 49) Service Level Agreements with third-party providers.

The only third-party provider critical to business operations is the outsourced hosting provider Memset.

Abintegro has an SLA in place with this provider and has successfully worked with Memset since June 2010.

### 50) Protecting and monitoring the physical infrastructure where processing is performed and data is stored.

We use two UK data centre facilities, one on either side of Reading, Berkshire, England. Both have state-of-the-art facilities, first-class connectivity and are manned 24/7 with skilled personnel.

There is a 24/7/365 on-site security presence with 24/7 internal CC-TV monitoring. In addition there are comprehensive security procedures including proximity access control.

Both data centres have independent dedicated gigabit fibre uplinks which take different routes to central London, one into Telehouse North and one into Telehouse East. From there the connections are peered with all the major UK backbones.

As part of the service we keep hot-standby equipment ready in the data centre to be used in the event of a major failure of a server. This means that if, for example, our servers were to suffer a major hardware failure we would be able to swap the disks into a spare chassis and have the server up and running again very rapidly and with minimal disruption.

In addition, our dedicated servers are equipped with RAID(6) disk mirroring which means that in the event of a hard disk failure (the most common component to fail) our servers will just keep running and our technicians will be alerted so that they can schedule a replacement.

More information can be found here:

Security, standards and accreditations: http://www.memset.com/about-us/security.php

ISO certification: http://www.memset.com/about-us/iso-certificates.php

Data centre: http://www.memset.com/about-us/datacentre.php

System server(s) monitoring: 24x7 server monitoring from over 20 locations world-wide, automated server reboots if unresponsive after 10 minutes, automatic notification via email and SMS to IT Director and Management Team.

Application monitoring: Automated application process testing every 5 minutes (24x7) with automatic notification via email and SMS to IT Director and Management Team.

### 51) System redundancy.

**Power**

As well as short-term Uninterruptible Power Supply (UPS) systems there are multiple diesel generators at both hosting sites, with a minimum of 96 hours fuel on-site, providing robust protection from power failures.

**Hardware**

We use high-quality hardware in order to minimise the risk of failure. All of our dedicated servers also use RAID, providing additional resilience against disk failures. We also keep hot-standby equipment on-site so that even in the most catastrophic server failure event we can simply swap the disks into a new, identical chassis.

**Security**

There is a 24/7 on-site security presence with 24/7 internal CC-TV monitoring. In addition there are comprehensive security procedures including proximity access control.

Additionally, since Memset do not offer colocation, only a small number of authorised personnel have access to our portion of the data centres and your servers.

**Maintenance**

All critical systems, such as UPS, generators and backup network links are tested on a regular basis to ensure that they are ready in the event of a real failure.

**Network connectivity**

Both data centres have independent dedicated gigabit fibre uplinks which take different routes to central London, one into Telehouse North and one into Telehouse East. From there the connections are peered with all the major UK backbones.

The two sites also have a gigabit fibre between them so if any one link fails data is automatically routed around the other two sides of the triangle.

Within the data centres we also ensure that there is no single point of failure up until the connection reaches our server. To do this we double-up on equipment such as routers, switches and firewalls in a mirrored configuration with a heart-beat monitor between the two sets.

**Business Continuity Management**

Business Continuity Management (BCM) process: The following stages outline the events undertaken in a business continuity situation.

| Stage | Description | Action | Owner | Time |
|---|---|---|---|---|
| System Issue Identification | Monitoring service detects server(s) or application issue (automated issue validation detection to minimise false positives) | Automated alerts via SMS, email to Abintegro IT Director and Management Team | Abintegro | 5 minutes (24/7/365) |
| Server Reboot | Automated server reboot | Automated reboot - after 10 minutes of server failure to respond | Host (Memset) | 10 minutes (24/7/365) |
| Hardware Failure | Server hardware failure | Replacement of faulty hardware once cause isolated | Host (Memset) | 120 minutes (24/7/365) |
| Application | Core application process | 1) Manual or Automated | Abintegro | 1) 30 minutes |

| | | | | |
|---|---|---|---|---|
| Failure | failure but hardware operational | monitoring reboot - after consecutive application process failures<br>2) IT diagnostics | | (24/7/365)<br>2) 3 hours 8.30am to 5.30pm (GMT), 7 days |
| Host Failure | IT host (Memset) cannot be reached/no longer available | Memset confirm cause of issue and resolution estimate | Host (Memset) | 60 minutes (24/7/365) |
| DNS Change | Requirement to change the DNS settings for the application to switch to backup servers if host failure | 1) *Automatic**, 2) Manual method to action DNS change to direct web traffic to backup server | Abintegro & Client where application runs on Client domain | 1) 3 hours (24x7)<br>2) 3 hours 8.30am to 5.30pm (GMT), 7 days |
| Backup Server Testing | Ensure application running correctly on backup server | 1) Automated testing<br>2) Manual testing | Abintegro | 1) 5 minutes (24/7/365)<br>2) 60 minutes 8.30am to 5.30pm (GMT), 7 days |

**Where client owns and manages the domain and requires 24x7 response*

- Business Continuity Management (BCM) service level:

1) Where automated DNS instruction issued: 3 hours (24x7)
2) Where manual DNS instruction issued: 3 hours 8.30am to 5.30pm (GMT), 7 days

Data recovery

The system (application code and user data) is encrypted (AES encryption using industry standard component) and backed up automatically daily (to a secure network filestore) with a rolling 7-day storage. Backups are restored as necessary as part of the working practice of the technology team. In practice this means backups are restored at least once a month.

Backups are taken specifically for: Web application files, databases, server configurations. All backups run daily. Backups are restored as necessary as part of the working practice of the IT team. In practice this means backups are restored at least once a month.

Memset backup services are electronic/disk-based backups with no physical movement of storage media. Backups are stored on both the Abintegro dedicated servers and separately on a secure network filestore with multi restore point capability.

Data backups are generated and encrypted (AES encryption) using industry standard component.

## 52) Administration of the production servers.

This service is managed by the Abintegro System Administrator and is configured with administrator and users account profiles. Only the administrator account can install additional programs / services specifically necessary for the business purpose. Designated users can manually request administrator account access to perform specific administrator activities and for defined periods of time. All access is authorised and monitored by the Abintegro IT Director and all users are assigned unique usernames and passwords. All  user activity is tracked via Windows system logs.

All application changes are made via SFTP. All changes/activity is stored on the SFTP server logs permitting full audit of changes made to the application.

Passwords are generated via a secure password generator with a minimum of 15 characters including alphanumeric characters, capitalisation and symbols.

### 53) Monitoring production servers and applications.

System server(s) monitoring: 24x7 server monitoring from over 20 locations world-wide, automatic notification via email and SMS to IT Director and Management Team.

Application multi-step transaction monitoring: Automated application process testing every 5 minutes (24x7) with automatic notification via email and SMS to IT Director and Management Team.

Real-time database, application and server monitoring providing complete visibility of performance, code/query issues and responsiveness.

Configuration checks are carried out at least annually, ensuring best practice server hardening is maintained.

### 54) Escalation procedure in case of a production failure.

Production system failures can be escalated from within the Abintegro client or technology teams and follow a documented process. Both teams work together both resolve the issue and communicate appropriately with clients. Scheduled outages are informed to clients by email. Unscheduled outages are communicated to clients by email or phone based on the nature and impact of the outage(s). All security incidents are the responsibility of the IT Director, or designated replacement, and remedial action is assigned to specified members of the technology team.

### 55) Problem management and root cause analysis.

Real-time, systematic, application, database and server monitoring/alerting.

### 56) Anti-virus protection.

All systems on the network have Sophos Antivirus with auto-update activated.