Use of Exchange Mail and Diary Service
Code of Practice

Introduction
This code of practice outlines the support mechanisms in place for the security of the Exchange mail and diary service. References are made to Active Directory, university’s Mail Relays and the university’s computing regulations. This code of practice is intended to support the Information Security Policy of the University and should be read in conjunction with that document.

1. Code of Practice Version

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>CoP Version</th>
<th>Template Version</th>
<th>Author</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>28/05/2012</td>
<td>Version 1st Draft</td>
<td>Version 1.4</td>
<td>Stephen Smith</td>
<td>Initial 1st Draft.</td>
</tr>
<tr>
<td>01/02/2013</td>
<td>Version 1.0</td>
<td>Version 1.4</td>
<td>Stephen Smith</td>
<td>Interim review</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>QA Date</th>
<th>QA Process</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>29/05/2012 to 12/06/2012</td>
<td>Review internally by Technical Staff and IS Apps leaders prior to presenting back to the IS Security Working Group.</td>
<td>Technical staff QA – 2 minor amendments to the system description applied.</td>
</tr>
</tbody>
</table>

Suggested date for Revision of the CoP | Author
01/02/2013 | Stephen Smith

2. System description

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>System Version</th>
<th>Author</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>29/05/2012</td>
<td>Exchange 2007 (SP3)</td>
<td>John McFarlane</td>
<td>The system’s service pack is regularly reviewed with any rollups tested and scheduled for live deployment following the service strategy for patching. Communications and alerts are managed accordingly within IS and following the standard IS model for planned system events.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.1 System name</th>
<th>Microsoft Exchange 2007 (SP3)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>2.2 Description of system</th>
<th>Exchange provides email, diary scheduling, shared contacts and delegable task lists to staff, staff visitors and research graduates. Users can access their emails and schedules securely with their preferred client interface (i.e. Outlook, Thunderbird, Mac Mail, Active Sync and Blackberry).</th>
</tr>
</thead>
</table>
### 2.3 Data

**Person:**
University User Names, Forename and Surname, Organisational Unit and Job Title.

Some preference settings defined by the users are kept with the account so that these are supplied to the user wherever they connect.

**Core data handled by the system:**
Email messages, scheduling data, contact lists and delegable task lists.

### 2.4 Components

**Core System:**
- Exchange 2007 (operating between 2 sites)
- Internet Security and Acceleration (ISA) System (back-office security of connections through the system)
- Hub Transport (mail transport and protocols in and out of the system)
- Client Access Server (CAS) (Load Balanced and Resilient)
- Fileshare Witness Server (synchronisation between sites)

**Dependencies on other systems:**
- Active Directory (includes Domain Controllers) – applies the frontline security allowing users to authenticate their credentials with the service.
- University of Edinburgh Mail Relays
- University of Edinburgh Network

**Other systems depending on Exchange:**
- Blackberry Enterprise System
- Davmail Gateway
- Data Protection Manager (DPM)

### 2.5 System owner
The system is owned and managed by the Multimedia and Communications team of IS Applications Service Management.

### 2.6 User base
The user base who are entitled to use this service for free are:
- All Staff
- All Staff Visitors
- All Research Graduates

### 2.7 Criticality
The Exchange system is a top priority service and considered business critical because it stores and handles emails, schedules, tasks and contacts on behalf of all users of the system.
2.8 Disaster recovery status

As a top priority service, Exchange uses the IS Alerts and call escalations process for critical escalation in the event of disaster.

The Exchange System continuously replicates and synchronises data between sites. In the event of a failure at the primary site, automated failover processes are in place to ensure continuity of service. Although the mail service can be recovered locally from this replication, DPM offers an extra layer of protection in the event of a disaster.

The system includes Data Protection Manager (DPM) owned and managed by ITI Architecture. This facility backs up the underlying Exchange system on a regular basis with the recovery process documented and tested. In the event of disaster affecting the automated failover and full recovery of the service would be initiated involving various parties in IS and potential external 3rd parties as appropriate.

As well as DPM, Exchange also relies heavily upon the operation of the Active Directory (including Domain Controllers), Mail Relays and the University Network to ensure this system remains fully operational and available to users. Disaster Recovery plans for each of these systems must also be considered with the Exchange system plans.

3. User responsibilities

3.1 Data

Users are required to protect their password to access the system. They are also governed by the computing regulations and applicable law to ensure data protection principals are adhered to when exporting or forwarding personal data to other mail services.

3.2 Usernames and passwords

Exchange uses Active Directory for authentication. The Active Directory code of practice should be referred to.

Users should never write down their password or give out their password to anyone else.

Users should never include passwords in emails or reply to emails asking for such details. IS staff will not ask for a user’s password in an email.

3.3 Physical security

Users are required to protect University data being transported away from the system by means of portable, physical storage device. They are also governed by the computing regulations and applicable law to ensure data protection principals are adhered to.
3.4 Remote/mobile working

Users may access Exchange using mobile devices or computers connecting via public networks or WiFi services. Users should configure a passcode to gain access to and use the device, and set an idle timeout (e.g. 1 minute) that will automatically lock the device when not in use. This helps prevent unauthorised access to data. More details about mobile device security connecting to University IT Services is at: http://www.ed.ac.uk/schools-departments/information-services/services/computing/desktop-personal/security/mobile-devices

Users must provide private credentials in order to connect to the email system and the data is encrypted between the system and connecting device.

When users login via a web browser the system can be made public aware allowing it to close unwanted user sessions more swiftly. The system also prompts users to close their web browser when they logout.

Users using this service from a public place should utilise these additional security features provided by the service.

3.5 Downloads and removal of data from premises

The University’s policy on storage, transmission and use of personal data and sensitive business information out with the University computing environment applies.

There are no system restrictions that would prevent users from downloading data via their own account.

3.6 Authorisation and access control

Accounts are created automatically in accordance with IS service entitlements policy. All users entitled to an account on Exchange may access their own account and may also permit other users of the service view or edit access (i.e. delegated access) as required. Any action taken by the delegate is auditable by the system and visible to recipients (i.e. “…sent on behalf of”).

By default the system does not allow any user to send emails on behalf of another users email account.

Only IS Staff are permitted administrator privileges in order to support users accordingly. Access is granted to staff when authorised by a senior member of staff in IS. IT staff must abide by university regulations when handling users accounts and data.

3.7 Competencies

Staff should be aware of the computing regulations.

4. System Owner Responsibilities
### 4.1 Competencies

Systems staff in IS Applications along with our infrastructure and network providers in ITI are all skilled and trained technically to support the security of our Exchange system.

Skills and expertise may vary between IS teams depending upon which component the team is responsible but includes the following key areas in order to help keep our Exchange system secure:

- Network traffic monitoring
- Identifying unusual patterns in data usage and connections
- Firewall configuration
- Mail relays (including mail routing messages onto Exchange)
- Active Directory and domain control configuration
- Internet Security and Acceleration (ISA) Server
- Server patching
- Email and Ediary connection protocols

### 4.2 Operations

The system is continuously monitored and alerts on standby in the event of any identifiable threat to the integrity or security of the system. Schedules are also in place for regular patches to operating systems and server software. Latest service packs are reviewed and scheduled from the point these become available.

Exchange also relies upon Active Directory, Mail Relays and the University Network. The code of practice for these systems should also be considered.

### 4.3 System documentation

Service level documentation and Self-help guidance for all users is published on the IS website. Service level documentation is owned and maintained by IS Service Management. All user topics are owned and maintained by IS User Services.

Systems documentation along with service level procedures are located in the collaborative tools section of the IS wiki (Insite).

Internal user support documentation is located on the User Services knowledge base.

### 4.4 Segregation of Duties

IS Technical and Support staff have administrator privileges on the system as described in 3.6 above.

IS Applications Technology Management permit access levels on requests authorised by senior IS staff only.

All users login to the system via Active Directory which is run and managed by IS ITI Architectures.

### 4.5 Security incidents

Security incidents are raised with IS IRT team to take the appropriate action.

### 4.6 Fault/problem reporting

Significant faults arising with the service may raise an alert automatically with the technical team for a quick response.

All enquiries or problems being reported should go via IS Helpline in the first instance.
4.7 Systems development

Smaller developments (i.e. 1 – 10 days effort) such as service improvements are prioritised and managed through service calls between IS teams and the business accordingly. All planned changes are communicated, documented in our change control system and any known user impact is published to IS alerts, news feed and twitter.

Larger developments (10 days or more effort) are managed through a project cycle (following PRINCE 2 methodology). A range of online project tools and templates provide a framework for managing new developments. All work is quality checked by project stakeholders at key stages of the project.

Any changes being applied to the Exchange system are tested in a test environment before being deployed onto the live systems.

5. System Management

<table>
<thead>
<tr>
<th>5.1 User account management</th>
<th>User accounts are created and managed automatically according to IT service entitlement and identity ageing policies. Gold copy master systems (i.e. HR system and Visitor Management System, EDDIR, Org Hierarchy) trigger the identity management processes centrally. Exchange connects to the Identity Management System which sources and notifies the identity data with any changes associated to each account. Exchange relies upon the Active Directory system in order to provision user accounts. Refer to the code of practice for the Active Directory system also.</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2 Access control</td>
<td>Admin level access is granted following a manual process as described in 3.6 and again in 4.4 above. Users entitled to use the service are granted user level access to their own accounts automatically. Users (or owner of an account) can permit other users to view mail folders, send mail on behalf of the owner, or manage the schedule of the owner. This is known as delegate access. Any interaction by the delegate is audited by the system and is visible to recipients of mail messages or meeting invites accordingly. All access to the system is automatically controlled according to IT service entitlement and identity ageing policies as described in 5.1 above.</td>
</tr>
</tbody>
</table>
5.3 Access monitoring
Logs track all messaging and usage through the system. Logs are replicated to a separate physical site and backed up along with messages and accounts data (including the unique identifier of the account).

5.4 Change control
A change control system and alerts publication records any changes applied to the live system.

5.5 Systems clock synchronisation
Time synchronisation is controlled from the Active Directory system. Refer to code of practice for the Active Directory system also.

5.6 Network management
All network activities are carried out by ITI Networks. Refer to the code of practice for University network systems also.

5.7 Business continuity
Data is continuously replicated through each day and held up to 7 days. In the event of a system failure users are switched over to the replica site. Databases on the live site are then built from the Data Protection Manager system before users are switched back to the live site. Communications with support staff and alerts are published throughout.

5.8 Security Control
Exchange comes with Internet Security and Acceleration (ISA) Servers which can apply back-to-back firewall capabilities, Virtual Private Networks, advanced application and web filtering, intrusion detection, client access rules and more. The system monitors, logs and alerts session activity, connectivity status across connection protocols and various levels of Exchange performance.

Exchange relies upon the PIX firewalls applied to the University network owned and managed by ITI Network Services. Refer to the code of practice for those systems accordingly.

6. Third Party

6.1 Outsourcing
N/A – The Exchange 2007 system operates entirely on-site.

6.2 Contracts and Agreements
Exchange complies with the agreed Microsoft campus and SELECT licenses purchased by the University.

All server-side licenses are installed and up-to-date.

ITI Architectures section owns and manages the University account agreed with our Microsoft supplier.

6.3 Compliance with the university security policy
N/A – Covered by this CoP and complies with University governance and Policies.

6.4 Personal data
N/A – Covered by this CoP and complies with University governance and Policies.