Use of Kx
Code of Practice

Introduction
This code of practice is intended to support the Information Security Policy of the University and should be read in conjunction with this document.

http://www.ed.ac.uk/schools-departments/information-services/about/policies-and-regulations/security-policies/security-policy

This code of practice is also qualified by The University of Edinburgh computing regulations, found at:

http://www.ed.ac.uk/schools-departments/information-services/about/policies-and-regulations

1. Code of Practice Version

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>System Version</th>
<th>Author</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/11/12</td>
<td>Kx2011.1 SP3.1</td>
<td>Sandy Agnew</td>
<td>Initial document</td>
</tr>
<tr>
<td>14/05/13</td>
<td>Kx2013 SP Edinburgh</td>
<td>Sandy Agnew</td>
<td>System upgrade 14/5/2013</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>QA Date</th>
<th>QA Process</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>27/06/2013</td>
<td>IT Security Working Group</td>
<td></td>
</tr>
</tbody>
</table>

Suggested date for Revision of the CoP

<table>
<thead>
<tr>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sandy Agnew</td>
</tr>
</tbody>
</table>

2.1 System name

Kx
2.2 Description of system

Kx is package provided by KSL for the specific purpose of student accommodation administration, conference organisation and hotel provision. It is delivered through Microsoft SQL Server and IIS platform and integrates with a range of University services such as Student Record Central Finance, and external bodies such as WPM and WorldPay.

**Core Modules**
- Catering
- Events
- Marketing
- Residential
- Student
- Web Applications
- Configuration
- Finance Interfaces

**Web Systems**
- Delivered Catering UoE facing
- Bed and Breakfast UoE facing
- Bed & Breakfast public facing
- Summer flats availability
- KxRegistration
- Student Applications
- Student Contracts
- KxE-induction
- Student Homes group availability

2.3 Data

- Person data for students
- Person data for external commercial customers
- Person data for internal customers
- Stock
- Product Prices
- Event Locations

2.4 Components

**Live environment**
- 2 SQL data base servers
- 1 SQL witness server
- 1 virtual Web server
- 2 SAN’s

**Test environment**
- 2 SQL data base servers
- 1 virtual witness server
- 1 IIS web server
- 2 SAN’s

With interfaces to SITS, Worldpay/WPM and E-Financials

2.5 System owner

Assistant Director Support Services Accommodation Services
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2.6 User base | **Core Modules**  
- ‘Super Users’ with access to configuration for specific modules  
- ‘User’ read and write access to specific modules but no access to Configuration  
- ‘User’ read and print restricted reports access only  
  
**Web**  
- ‘Internal users’; with authorised rights to buy products using the e-it system  
- ‘External users’ paying for goods and services using, WPM Gateways or by invoice |
| 2.7 Criticality | High |
| 2.8 Disaster recovery status | DR is delivered through the availability to fail over to a mirrored database maintained at a separate physical location. Documentation of fail over process is maintained by IS Production Management |
## 2. User responsibilities

### 3.1 Data
- Super Users’ with access to configuration for specific modules
- ‘Users’ read and write access to specific modules but no access to Configuration. Will have access to sensitive user data
- ‘Users’ read and print access only with no access to sensitive data
- Level of access must be authorised by line manager
- Access to system configuration must be authorised by an Assistant Director

### 3.2 Usernames and passwords
A single username and password is used. Users are responsible for maintaining the security of their user name and password. The system does not force password changes.

### 3.3 Physical security
Users are not required to take any responsibility for the security of the system other than to ensure the security of their login details. No specific guidance is given regarding security of their PC’s.

### 3.4 Remote/mobile working
Access to systems is through the UoE VPN service.

### 3.5 Downloads and removal of data from premises

### 3.6 Authorisation and access control
Level of access is determined by user’s manager other than access to configuration which can only be authorised by Assistant Director or above.

### 3.7 Competencies
Business and system knowledge is delivered through training. Customarily use of a similar or the same system is, in general a job requirement.
### System Owner Responsibilities

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>4.1 Competencies</strong></td>
<td>The system owner has a knowledge of the business processes that the system supports</td>
</tr>
</tbody>
</table>
| **4.2 Operations** | Principle mechanisms for ensuring security are:  
  - The user access authorisation process.  
  - Procedures and on line request forms are on AS intranet  
  - IS are responsible for the overall security of the data on AS servers  
  - AS servers are part of the IS Microsoft Critical Patching schedule |
| **4.3 System documentation** | System documentation  
  - User manuals hard copy and on-Line  
  - Fail over procedures procedural – Form part of AS/IS SLA  
  - Fail over procedures technical – retained by IS Production Management |
| **4.4 Segregation of Duties** | **Core Modules**  
  - ‘Super Users’ with access to configuration for specific modules  
  - ‘Users’ read and write access to specific modules but no access to Configuration  
  - ‘Users’ read and print access only  

  Managers determine access rights with the exception of configuration which requires the authorisation of an Assistant Director or above  

  **Web**  
  - ‘Internal users; with authorised rights to buy products using the e-it system. User access determined by rights already assigned through the e-it system.  
  - ‘External users’ paying for goods and services using WPM Gateways or by invoice. Users do not require authorisation to buy goods and services on line as payment is made in advance by credit card |
| **4.5 Security incidents** | Currently any security incident would be addressed by the removal of access rights until the situation is investigation and resolved. |
| **4.6 Fault/problem reporting** | Following reference to a Super User, faults are reported by users directly to the third party supplier, KSL, who is responsible for support |
| **4.7 Systems development** | Driven by business needs from all levels of the business. When appropriately authorised, a requirement can be met through either a piece of bespoke work or the inclusion of the work in a future release of the software |
4. **System Management**

<table>
<thead>
<tr>
<th>5.1 User account management</th>
<th>New accounts are created on request from identifies managers for modules for which they are responsible. Accounts are ceased on request from a manager. Where this request has not been made, a monthly list of ‘leavers’ is received from internal HR and any accounts that are still active are ceased</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2 Access control</td>
<td>Level of access is determined by manager</td>
</tr>
<tr>
<td>5.3 Access monitoring</td>
<td>There is no mechanism to detect unauthorised access of any module</td>
</tr>
<tr>
<td>5.4 Change control</td>
<td>Any changes to the Live system are subject to the completion of a Change Control Request submitted by KSL and reviewed by IS Applications</td>
</tr>
<tr>
<td>5.5 Systems clock synchronisation</td>
<td>IS are responsible for this activity</td>
</tr>
<tr>
<td>5.6 Network management</td>
<td>This is the responsibility of IS Network Services</td>
</tr>
<tr>
<td>5.7 Business continuity</td>
<td>Business continuity is provided by the mirrored fail over infrastructure</td>
</tr>
<tr>
<td>5.8 Security Control</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### 5. Third Party

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1 Outsourcing</td>
<td>Security of the data is not shared and is the responsibility of UoE</td>
</tr>
<tr>
<td>6.2 Contracts and Agreements</td>
<td>Contract with supplier for the maintenance and support of the core modules and web sites as described in section 2.2. This is a rolling contract renewable on an annual basis through the payment of support, licencing and maintenance charges.</td>
</tr>
</tbody>
</table>
| 6.3 Compliance with the university security policy | The company who supplied and support Kx has not been asked to comply with the university security policy and this CoP. Potential Risks through the deliberate or accidental sharing of university data with an unauthorised company or individual:  
  
- Financial loss  
- Reputational damage  
- Financial penalty |
| 6.4 Personal data | When personal data is shared, for hosting purposes, the supplier is required, as per Records Management, to enter into a standard data protection agreement for the transfer of Personal Data from the University of Edinburgh (as Data Controller) to a Data Processor within the European Economic Area |