Confidential Information Held by the School of Computer Science

Date: 6/9/2013  
Author/Contact: Tom Chothia  
Classification: Open

Executive Summary: This document lists the types of confidential data held by the School of Computer Science, University of Birmingham. It also lists main risks, users, owners and controls associated with each type of data (the controls and end of use for each form of data would normally be listed in a separate document, and are only listed here as a temporary measure).

Scope: This document lists only data held by the School of Computer Science that is considered to be “Confidential” according to the Universities data classification criteria. It is not a full asset register: it does not list important physical assets, and it does not list information assets that would not be classified as confidential.

Version History:

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>20/8/2013</td>
<td>1.0</td>
<td>Tom Chothia</td>
<td>Initial version</td>
</tr>
<tr>
<td>6/9/2013</td>
<td>1.1</td>
<td>Tom Chothia</td>
<td>Added section on restricted data</td>
</tr>
</tbody>
</table>

Confidential Information:

Student welfare information:

Description: Information given to the school by students to support welfare claims.

Primary CIA property(s): Confidentiality.

Primary Risk: Personal medical information regarding students is made public, causing embarrassment to the student, breaching the data protection act and couring loss of reputation to the University.

Principal Users: School of computer science welfare team.

Owner: School of computer science welfare team.

Controls: All information stored in an encrypted database, access restricted to members of the School of Computer Science welfare team. E-mail only via the welfare@cs.bham.ac.uk or extenuating-circs@cs.bham.ac.uk e-mail addresses. Files stored encrypted and paper documents stored in a locked filing cabinet.

Live Exam Papers:

**Description:** Exam papers before the exam, in draft or final form.

**Primary CIA property(s):** Confidentiality, Availability, Integrity.

**Primary Risk:** Exam papers are found to have been leaked after an exam is taken leading to loss of reputation of the school.

**Principal Users:** Academic setting the paper, School admin staff, School Exam officer, quality assessment committee, module reviewers, external examiners.

**Owner:** School of computer science exam officer.

**Controls:** Stored encrypted, transported encrypted on USB sticks, may be transported by secure postal service, (under exceptional circumstances sent encrypted by e-mail).

**End of use:** Used exam papers will be made publicly available after the exam.

Unmarked Exam Scripts:

**Description:** Student’s exam scripts, while they are being marked and while the marks are being verified.

**Primary CIA property(s):** Availability.

**Primary Risk:** Exam scripts are lost, meaning that the School cannot award qualifications, as planned.

**Principal Users:** Academic marking the paper, School admin staff, University Exams Office.

**Owner:** School admin staff.

**Controls:** Paper copies only, kept in a locked room or locked filing cabinet, or other secure locations. May be transported by secure postal service.

**End of use:** Stored for 12 months then disposed of securely.

Password Hashes:

**Description:** Hashes of the passwords for all users of the system maintained by the school of computer science, checked every time a user logs in.

**Primary CIA property(s):** Confidentiality, Availability, Integrity.

**Primary Risk:** Password word hashes are leaked and cracked allowing remote access to users accounts.

**Principal Users:** All staff but only via the standard log in system, password reset tools.

**Owner:** School of computer science IT staff.

**Controls:** Stored securely in School’s Active Directory system. Accessed only via the standard log in system and password reset system. Admin restricted only to schools IT staff.

**End of use:** Securely deleted.
Confidential Data From Outside Organisations:

**Description:** From time to time an outside organisation may share confidential information with researchers from the school.

**Primary CIA property(s):** Confidentiality.

**Primary Risk:** Data is leaked, leading to lost of trust in the school and possibly financial damage (or other losses) to the outside organisation.

**Principal Users:** The academics involved in the research project in question.

**Owner:** The academic leading the research project in question.

**Controls:** As specified by the outside organisation.

**End of use:** As specified by the outside organisation.

Legal Documents:

**Description:** In the case that members of the school are involved in legal action some documents may be restricted by court order. The School may also be required to provide certain data when ordered.

**Primary CIA property(s):** Confidentiality, Availability.

**Primary Risk:** Leaking data or not being able to provide data when ordered may be considered contempt of court.

**Principal Users:** The academics involved in the legal action in question, head of school, the University’s Legal Services.

**Owner:** The lead academic involved in the legal action, or the Head of School in the case of action against the School.

**Controls:** Documents must be kept on a secure school system or encrypted.

**End of use:** Stored for future reference.
Restricted Information:

The school of computer science also has data that, if lost or leaked, would not have a *major* impact on the School or University, but should still be kept private. This kind of data is classed as restricted, rather than confidential and includes:

Student’s marks, salary information, outcomes of staff performance development reviews, job applications and CVs, School strategy documents, School financial information, private keys for the schools web server certificates, contracts with outside businesses, personal information not relating to race, religion, medical issues etc, some unpublished research, committee minutes.

This data should not be made public by for instance publishing it on an unprotected website, however it does not need to be encrypted when at rest (e.g., stored on a computer or device) or in transit (e.g., sent by e-mail).