Information Technology

**PRIVACY:**
Paul Hancock, Access and Privacy Manager
paul.hancock@ubc.ca, 604-822-2451

**SECURITY:**
Alan Tromba,  Senior Systems Analyst
alan.tromba@ubc.ca, 604-827-1410

# Key Security and Privacy Risks and What “Good” Looks Like

Information Security and Privacy staff have identified a number of commonly occurring risks for personal information and other confidential information. We have captured these risks below and provided guidance on “What Good Looks Like”.  During the development of all new systems, initiatives or projects, we strongly recommend you consider the following, along with the Information Security Standards (**http://cio.ubc.ca/securitystandards**) and the Privacy Fact Sheets (**http://universitycounsel.ubc.ca/access-and-privacy/privacy/).** We are happy to assist you with any questions that may arise as you work through the development process.

| | **Risk Area** | **What “Good” Looks Like** | **Relevant Information Security Standard (ISS) or Privacy Fact Sheet (PFS)** |
|---|---|---|---|
| **Privacy** | Personal information collected without authorization. | Personal information may usually only be collected if it is necessary for an operating program or activity of UBC. | PFS: “Collecting Personal Information” |
| | Personal information collected without a privacy notification. | A privacy notification must be provided whenever personal information is collected. | PFS: “Collecting Personal Information” |
| | Personal information stored outside Canada (e.g. using cloud services) | Personal information must not be stored outside Canada or accessible from outside Canada unless you have the informed written consent of the affected individuals. | PFS: “Overview of Privacy” |
| | Personal information used without authorization. | Personal information must only be used for the purpose it was collected, or a consistent purpose. | PFS: “Overview of Privacy” |
| | Personal information disclosed without authorization. | Personal information may be shared within UBC based on the “need to know” principle. Personal information must not be shared outside UBC without the consent of the affected individuals, or approval from the Access and Privacy Manager. | PFS: “Overview of Privacy” |
| | Personal information not stored long enough / too long. | Personal information must be retained for at least one year after it is used to make a decision that affects the individual. After one year, personal information must be deleted when it is no longer required. | PFS: “Overview of Privacy” |
| **Security** | Anti-virus not installed on systems. | All systems (including Linux-based systems) should have managed anti-virus installed. | ISS #14 |
| | Vulnerability tests not performed on systems. | Vulnerability scans should be conducted before going live and after major changes and medium and high vulnerabilities be remediated. | ISS #14 |
| | Timely patching of systems (operating system and application) not performed. | All systems should be part of a managed patch management regime for applications and operating systems. | ISS #14 |
| | Web & database servers not separated. | All web facing applications are separated from the database server (not running on the same server/system) | ISS #19 |
| | 3rd parties engaged without requiring formal acceptance of UBC privacy and security requirements. | Confidentiality agreements must be signed and 3rd party assessments must be performed. | ISS #9 |
| | Outdated security certificate technologies being used. | All confidential information should be transmitted via the web using HTTPS with TLS 1.0 as a minimum. | ISS #16 |
| | Lack of role-based access to data and / or inappropriate access rights assigned. | Access to confidential data should be granted using role based access controls and permissions set following principle of least privilege. | ISS #9, 11, & 19 |
| | Systems not hardened. | All systems should have all redundant services and ports deactivated to reduce the risk of vulnerabilities being exploited. | ISS #14 |