THE UNIVERSITY OF BRITISH COLUMBIA

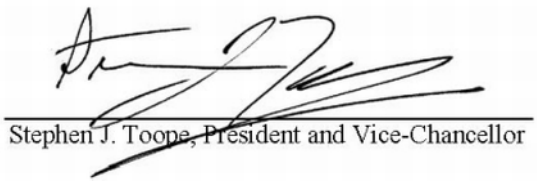
Report to the Board of Governors

SUBJECT **AMALGAMATION AND AMENDMENT OF POLICY #104 (RESPONSIBLE USE OF INFORMATION TECHNOLOGY FACILITIES AND SERVICES) AND #106 (ACCESS TO AND SECURITY OF ADMINISTRATIVE INFORMATION)**

MEETING DATE **June 4, 2013**

Forwarded to the Board of Governors on the
Recommendation of the President

APPROVED FOR SUBMISSION



Stephen J. Toope, President and Vice-Chancellor

Presented By Hubert Lai, Q.C., University Counsel

Oliver Gruter-Andrew, Chief Information Officer, IT

Report Date May 10, 2013

DECISION REQUESTED

IT IS HEREBY REQUESTED that *the UBC Board of Governors repeal Policies #104 (Responsible Use of Information Technology Facilities and Services) and #106 (Access to and Security of Administrative Information) and approve the proposed new Policy #104 (Acceptable Use and Security of UBC Electronic Information and Systems) (the "Policy"), effective immediately*

EXECUTIVE SUMMARY

The proposed Policy combines two existing policies. It clarifies the responsibilities of faculty, staff and students with respect to the acceptable use of University electronic information and the services, devices and facilities that store or transmit this information. It also enhances the security of the University's information assets by establishing a framework for the creation of security-related procedures (called Information Security Standards).

The proposed Policy has been developed by a Policy Review Committee under the oversight of the Office of the University Counsel. The policy creates no legal or governmental liabilities.

Approval of the Policy is within the statutory powers of the Board of Governors and no governmental approvals are required.

Place and Promise COMMITMENT(s)	The proposed amendments to the Policy support: • The Outstanding Work Environment commitment - provide a fulfilling environment in which to work, learn, and live, reflecting our values and encouraging the open exchange of ideas and opinions. • The Research Excellence commitment - create and advance knowledge and understanding, and improve the quality of life through the discovery, dissemination, and application of research within and across disciplines.
Place and Promise ACTION(s)	In support of the commitments to outstanding work environment and research excellence, the proposed amendments to the Policy: • Ensure that academic and administrative heads and directors have the training, time and support they require to be effective • Increase coordination of mid-level plans to provide a respectful, inclusive and collegial work environment • Enhance infrastructure to support leading edge research
Description & Rationale	Policy #104, which governs responsible use of the University's Information Technology facilities and services, was approved in November 2000 and has never been substantively revised or amended. Policy #106, which regulates access to and security of Administrative Data, was first approved in January 2001 and has also never been substantively revised or amended, although minor amendments to the Procedures were authorized by the President in July 2010. Users across the University have asked for various aspects of these policies to be clarified or elaborated. In particular, the following important changes have been made: 1. Even though Policies #104 and #106 are closely related, the terminology and scope of the two policies are inconsistent. Consequently, the two policies have now been rationalized and amalgamated into one policy. 2. The current policies only apply to faculty, staff, and students, but not to other individuals who may have access to University systems. The proposed Policy fills this gap by broadening the scope to any individuals who have access to UBC Electronic Information and Systems. 3. The current policies do not deal uniformly with all types of University electronic information. The proposed Policy rectifies this by providing a common framework for the appropriate use and security of all electronic information used to conduct University business (administrative, academic and research). 4. The current Policy #106 does not explicitly require users to comply with guidelines developed by the Chief Information Officer on the security of UBC information and systems. The proposed Policy addresses this omission by requiring all users to comply with Information Security Standards, which are developed by the CIO with the input of an Advisory Committee. Some of these Standards have already been drafted, and more will be prepared over the coming months.

5. The current Policy #104 allows for incidental personal use of facilities or services, under limited circumstances. The proposed policy continues to allow such use, and provides additional guidance about the balance between users' reasonable expectation of privacy and the University's right to access information stored on UBC systems under appropriate circumstances.

6. As it is unreasonable to expect the proposed Policy to apply to systems specifically designed for personal use, such as the University's student email system, the proposed Policy contains a mechanism enabling the CIO to approve separate terms of use for these systems. Upon such approval, the Policy will not apply to such systems.

FINANCIAL
Funding Sources, Impact on Debt Ratios

This proposed new Policy will not have a significant financial impact. Information Security Standards will be introduced in a carefully staged manner to minimize the impact upon resources.

SCHEDULE
Implementation Timeline

If approved, the proposed new Policy would take effect immediately. Information Security Standards will be introduced periodically over the coming months.

BENEFITS
Learning, Research, Financial, Sustainability & Reputational

- Clarifies inconsistencies and fills gaps in the current policies
- Guides the acceptable use of electronic information and systems
- Assists the University to protect all electronic information stored on its systems
- Establishes a mechanism for the creation of Information Security Standards, with input from a broadly representative advisory committee
- Implements a procedure for authorizing variances to Information Security Standards
- Enables the University to protect the privacy interests of users, while maintaining reasonable access to its systems and information

CONSULTATION
Relevant Units, Internal & External Constituencies

The Office of the University Counsel convened a policy review committee to undertake a comprehensive review of the Policy. The Policy Review Committee is comprised of the following members:

- Hubert Lai, University Counsel (Co-Chair);
- Paul Hancock, Access and Privacy Manager (Co-Chair);
- John Burton, Assistant Professor, Faculty of Management (UBC Okanagan);
- Larry Carson, Associate Director, Information Security Management, IT;
- Francisco Colino, Ph.D. student, Interdisciplinary Studies (UBC Okanagan);
- Oliver Gruter-Andrew, Chief Information Officer, IT;
- Caroline Haythornthwaite, Director, Library, Archival and Information Studies;
- Christopher Pryde, Director, IT Operations, Faculty of Medicine;
- Jennifer Stephens, Ph.D. student, Nursing;
- Don Thompson, Chief Technology Officer, IT (UBC Okanagan); and
- Michael Thorson, Director, Infrastructure

The Policy Review Committee prepared and presented the proposed Policy to the Board of Governors at its meeting on December 4, 2012. The proposed Policy was published for public comment on the Office of the University Counsel website and an email was sent to the "Heads Up" Email list regarding the Call for Comments. In response, nine respondents provided comments.

The Policy Review Committee reviewed all of the responses in detail, and made a number of changes to address the concerns raised by the University community. The Policy Review Committee unanimously supports the proposed amendments. A summary of the comments received is available in the attachments below.

Additional Materials

Attachment 1. Draft Policy Presented to the Board for Information on December 4, 2012

Attachment 2. Proposed Policy Being Presented to the Board for Approval

Attachment 3. Summary of Public Comments and Any Actions Taken

Attachment 4. Draft List of Systems Exempted from Policy 104

Attachment 5. Draft Information Security Standards

Previous Report Date	December 4, 2012	**Decision**	N/A
Discussion Points	N/A		
Action / Follow Up	Publication for public comment.		

Attachment 1: Draft Policy Presented to Board on December 4, 2012

The University of British Columbia Board of Governors	**Policy No.:** **104**	**Approval Date:** x **Last Revision:** x
	Responsible Executive: Vice-President, Academic and Provost Deputy Vice-Chancellor (UBC Okanagan)	

Title:

Acceptable Use and Security of UBC Electronic Information and Systems

Background & Purposes:

This policy is intended to outline the responsibilities of members of the University community with respect to the acceptable use and security of University electronic information and the services, devices and facilities that store or transmit this information.

The Responsible Executive may adopt standards and procedures consistent with this policy. In addition, faculties and departments may adopt implementation procedures that reflect local circumstances, provided they too are consistent with this policy.

1. General

1.1. Faculty, staff and students rely on UBC Electronic Information and Systems for academic, research and administrative purposes. Users of these resources are responsible for using them appropriately and maintaining their security.

1.2. The Chief Information Officer or delegate (the "CIO") shall perform a coordinating role in the implementation, administration, and support of this policy by:

1.2.1. providing guidance on compliance with the policy;
1.2.2. providing an ongoing security awareness program; and
1.2.3. assisting in the investigation of breaches of the policy.

1.3. If a User becomes aware that UBC Electronic Information and Systems are not being used appropriately, the User should bring this to the attention of the relevant administrative head of unit or to the CIO so that appropriate action can be taken to address the situation.

1.4. Users who breach this policy may be subject to the full range of disciplinary actions. In addition to any other sanctions that the University may impose in the event of a violation, the University may restrict or withdraw access to UBC Electronic Information and Systems, including computing privileges and network access.

1.5 The CIO may designate UBC Systems to which this policy does not apply. Where the CIO determines that such a designation is appropriate, the CIO must, in consultation with the Office of the University Counsel, approve separate terms of use that govern the use of the designated UBC Systems.

2. Acceptable Use of UBC Electronic Information and Systems

2.1. The University does not and will not attempt to limit the Academic Freedom of those who use UBC Electronic Information and Systems, provided that Users utilize these resources in a manner that is consistent with:

2.1.1. applicable laws, including but not limited to the Canadian *Criminal Code*, the Canadian *Copyright Act*, the B.C. *Civil Rights Protection Act*, the B.C. *Freedom of Information and Protection of Privacy Act*, and the B.C. *Human Rights Code*;
2.1.2. this policy and other applicable University policies, including but not limited to the Discrimination and Harassment Policy and the Records Management Policy;
2.1.3. collective agreements with faculty and staff; and
2.1.4. the terms of employment applicable to non-unionized staff.

2.2. UBC Electronic Information and Systems may only be used for their intended purposes. Incidental personal use of these resources is acceptable provided that such use:

2.2.1. does not interfere with the User's job performance; and
2.2.2. is not an unacceptable use as per paragraph 2.3 of this policy.

2.3. Unacceptable uses of UBC Electronic Information and Systems are any uses that disrupt or interfere with the use of the resources for their intended purpose. The following are representative examples of unacceptable uses:

2.3.1. engaging in illegal activities;
2.3.2. sending threatening, harassing or discriminatory messages;
2.3.3. misrepresenting the User's identity as sender of messages;
2.3.4. intercepting or examining the content of messages, files, or communications in transit;
2.3.5. infringing upon the copyright of computer programs, data compilations and all other works (literary, dramatic, artistic or musical);
2.3.6. infringing upon the legal protection provided by trademark law and the common law for names, marks, logos, and other representations that serve to distinguish the goods or services of one person from another;
2.3.7. making unauthorized copies of proprietary software, or offering unauthorized copies of proprietary software to others;
2.3.8. failing to maintain the confidentiality of passwords, access codes or identification numbers used to access UBC Electronic Information and Systems;
2.3.9. seeking information on passwords or information belonging to another User;
2.3.10. accessing or examining other Users' accounts, files, programs, communications or information;
2.3.11. destroying, altering, dismantling, disfiguring or disabling UBC Electronic Information and Systems;
2.3.12. damaging or altering the hardware or physical components of UBC Systems;
2.3.13. attempting to circumvent security controls on UBC Electronic Information and Systems;
2.3.14. knowingly introducing a worm or virus; and
2.3.15. engaging in any uses that result in the loss of another User's information.

2.4. Nothing in paragraph 2.3 shall be construed as preventing or restricting duly authorized system administrators or other technical personnel from carrying out their duties.

3. Security of UBC Electronic Information and Systems

3.1. All Users must comply with the Information Security Standards established under this policy regarding the acceptable use and security of UBC Electronic Information and Systems.

3.2. The CIO is responsible for:

3.2.1. developing and issuing the Information Security Standards, which must be consistent with this policy;
3.2.2. publishing the Information Security Standards on the UBC Information Technology web site for access by all Users; and
3.2.3. reviewing the Information Security Standards on a bi-annual basis or at such other interval as the CIO determines.

3.3. A committee (the "Advisory Committee") will be established by the CIO and will consist of representatives from the units responsible for maintaining and/or operating significant UBC Electronic Information and Systems, as well as a representative of the Office of the University Counsel. The Advisory Committee will provide advice to the CIO on the development of and ongoing updates to the Information Security Standards and will also provide advice to the relevant Responsible Executive with respect to any disagreements referred to him or her pursuant to paragraph 3.6 of this policy.

3.4. Academic and administrative units that wish to deviate from the Information Security Standards are required to request the authorization of the CIO before proceeding.

3.5. Where the Information Security Standards do not address the reasonable requirements of a unit's use of and access to UBC Electronic Information or Systems, the CIO may authorize a deviation or update the Information Security Standards as appropriate.

3.6. If a disagreement arises and cannot be resolved informally between the CIO and the head of an academic or administrative unit in respect of the requested deviation then either party may refer the disagreement to the relevant Responsible Executive, who will decide the matter. This Responsible Executive may consult with the Advisory Committee and/or the other Responsible Executive if he or she determines it would be appropriate to do so.

4. Use of Non-University Systems for University Business

4.1 To maintain the security of UBC Electronic Information, University business must only be conducted using UBC Systems, except as otherwise permitted by the Information Security Standards.

5. Privacy of Users

5.1. Since paragraph 2.2 of this policy authorizes the incidental personal use of UBC Electronic Information and Systems, the University recognizes that these resources may contain records relating to this personal use, e.g. personal emails, documents, internet use logs and voicemails (the "Personal Use Records").

5.2. While the University takes reasonable measures to back up information and protect it from loss, the University does not warrant that Personal Use Records will be retained in the UBC Systems or remain confidential. To protect their Personal Use Records from inadvertent destruction or disclosure, Users are encouraged to clearly mark them as personal, store them separately from UBC Electronic Information, and back them up on a regular basis.

5.3. While the University does not, as a routine matter, review Personal Use Records generated, stored, or maintained on UBC Systems, the University retains the right to inspect, review, or retain the Personal Use Records for legitimate University purposes. These purposes include, but are not limited to:

5.3.1. responding to lawful subpoenas or court orders;
5.3.2. investigating misconduct and determining compliance with University policies; and
5.3.3. searching for electronic messages, data, files, or other records that are required for University business continuity purposes.

5.4. Users should understand that electronic information does not necessarily disappear after it has been deleted. The University may, in accordance with paragraph 5.3 of this policy, retrieve or reconstruct records from UBC Systems, which may include Personal Use Records, even after they have been deleted.

5.5. Users should also be aware that the University routinely monitors network transmission patterns such as source/destination, address/port, flags, packet size, packet rate, and other indicia of traffic on its networks and systems. This routine monitoring may inadvertently reveal information about the personal use of the UBC Electronic Information and Systems.

5.6. Except in emergencies or other unusual situations, the University will seek the consent of a User before intentionally accessing his or her Personal Use Records. If the University is required to gain access without the individual's consent, such access must be authorized by the head of the relevant unit and the CIO, in accordance with the procedure set out in the Information Security Standards.

6. Administrative Responsibilities

6.1. Administrative heads of unit are responsible for establishing and maintaining UBC Electronic Information and Systems within their areas of responsibility. These responsibilities include:

6.1.1. ensuring that UBC Electronic Information and Systems are secured with adequate controls, with particular care concerning User identification and validation measures;
6.1.2. ensuring, as appropriate or required, that UBC Electronic Information within their area of responsibility is maintained, transmitted and stored in a secure and consistent manner that adheres to all relevant University policies and standards;
6.1.3. authorizing access for individuals to UBC Electronic Information and Systems within their area of responsibility;
6.1.4. renewing, retiring, and revoking User authorizations within their area of responsibility;
6.1.5. ensuring that a contingency plan, including appropriate data back-up systems and recovery systems, is being used within their unit;
6.1.6. ensuring that breaches of this policy occurring within their unit are resolved and/or referred to the CIO, as appropriate, and that where they are so referred, continuing to assist in the investigation;
6.1.7. ensuring that technical staff within their unit are aware of and adhere to this policy, and that they support University standards in the design, installation, maintenance, training, and use of UBC Electronic Information and Systems; and
6.1.8. taking immediate and appropriate action when they become aware of violations of this policy or its procedures.

7. Definitions

7.1. *Academic Freedom* is defined in the UBC Vancouver and UBC Okanagan calendars.

7.2. *Confidential* UBC Electronic Information is information that is highly sensitive. This includes, but is not limited to:

7.2.1. personal information (not including the name and business contact information of faculty and staff members);
7.2.2. financial information; and
7.2.3. information the release of which could reasonably be expected to harm the security of individuals, systems or facilities.

7.3. *Information Security Standards* means the standards established under this policy regarding the acceptable use and security of UBC Electronic Information and Systems. The Information Security Standards are published on the UBC Information Technology Office website at: http://www.it.ubc.ca/sites/it.ubc.ca/files/uploads/__shared/assets/UBC_Information_Security_Manual.pdf.

7.4. *Sensitive* UBC Electronic Information is information that is not Confidential, but cannot be released to the general public. This includes, but is not limited to:

7.4.1. information supplied in confidence;
7.4.2. research data that does not contain Confidential information;
7.4.3. information relating to plans, projects or proposals that have not been made public; and
7.4.4. contractually protected information, such as electronic library resources.

7.5. *UBC Electronic Information* is electronic information needed to conduct University business (administrative, academic or research).

7.6. *UBC Electronic Information and Systems* includes UBC Electronic Information and UBC Systems.

7.7. *UBC Systems* are services, devices and facilities that are owned or leased by the University, that are used for a University purpose, and that store or transmit UBC Electronic Information. These include, but are not limited to:

7.7.1. computers and computer facilities;
7.7.2. computing hardware and equipment;
7.7.3. mobile computing devices such as laptop computers, smartphones and tablet computers;
7.7.4. electronic storage media such as CDs, USB memory sticks and portable hard drives;
7.7.5. communications gateways and networks;
7.7.6. email systems;
7.7.7. telephone and other voice systems; and
7.7.8. software.

7.8. *Users* are faculty, staff, students and any other individuals who have access to UBC Electronic Information and Systems.

Attachment 2: Proposed Policy

The University of British Columbia Board of Governors	**Policy No.:** 104	**Approval Date:** x **Last Revision:** x
	Responsible Executive: Vice-President, Academic and Provost Deputy Vice-Chancellor (UBC Okanagan)	

Title:

Acceptable Use and Security of UBC Electronic Information and Systems

Background & Purposes:

This policy is intended to outline the responsibilities of members of the University community with respect to the acceptable use and security of University electronic information and the services, devices and facilities that store or transmit this information.

The Responsible Executive may adopt standards and procedures consistent with this policy, all of which are posted at http://cio.ubc.ca/securitystandards. In addition, faculties and departments may adopt implementation procedures that reflect local circumstances, provided they too are consistent with this policy.

The University is committed to the principle of academic freedom. This policy should be interpreted in that context.

Nothing in this policy should be interpreted in a manner that is inconsistent with the University's legal obligations, including its obligations under collective agreements with faculty and staff and the terms of employment applicable to non-unionized staff.

1. General

1.1. All Users of UBC Electronic Information and Systems are responsible for using them appropriately and maintaining their security.

1.2. The Chief Information Officer or delegate (the "CIO") shall perform a coordinating role in the implementation, administration, and support of this policy by:

1.2.1. providing guidance on compliance with the policy;
1.2.2. providing an ongoing security awareness program; and
1.2.3. assisting, where appropriate, in the investigation of breaches and potential breaches of the policy.

1.3. If a User becomes aware that UBC Electronic Information and Systems are not being used appropriately, the User should bring this to the attention of the relevant administrative head of unit or to the CIO so that appropriate action can be taken to address the situation.

1.4. Users who breach this policy may be subject to the full range of disciplinary actions. In addition to any other sanctions that the University may impose in the event of a violation, the University may restrict or withdraw access to UBC Electronic Information and Systems, including computing privileges and network access.

1.5 Records containing teaching materials or research information of persons teaching or carrying out research at the University are not subject to the B.C. *Freedom of Information and Protection of Privacy Act*. However, the University wishes to ensure that all UBC Electronic Information, including teaching materials and research information, is properly secured and the integrity of UBC Systems is maintained. Therefore, this policy applies to all UBC Electronic Information, except as otherwise provided by paragraph 1.6.

1.6 Where a UBC System is not intended to be used for University Business, the CIO must, in consultation with the Office of the University Counsel, approve separate terms of use that govern the use of such system. Upon such approval, this policy will not apply to such system.

2. Acceptable Use of UBC Electronic Information and Systems

2.1. UBC Electronic Information and Systems may only be used in a manner that is consistent with:

2.1.1. applicable laws, including but not limited to the Canadian *Criminal Code*, the Canadian *Copyright Act*, the B.C. *Civil Rights Protection Act*, the B.C. *Freedom of Information and Protection of Privacy Act*, and the B.C. *Human Rights Code*;
2.1.2. this policy and other applicable University policies, including but not limited to the Discrimination and Harassment Policy, the Respectful Environment Statement, and the Records Management Policy;
2.1.3. collective agreements with faculty and staff; and
2.1.4. the terms of employment applicable to non-unionized staff.

2.2. Incidental personal use of UBC Electronic Information and Systems is acceptable provided that such use does not interfere with the User's job performance and is not a prohibited use as per paragraph 2.3 of this policy. Except for the foregoing, these resources may only be used for University Business.

2.3. Prohibited uses of UBC Electronic Information and Systems are any uses that disrupt or interfere with the use of the resources for their intended purpose. The following are representative examples of prohibited uses:

2.3.1. breaching applicable laws or University policies;
2.3.2. sending threatening, harassing or discriminatory messages;
2.3.3. misrepresenting the User's identity as sender of messages;
2.3.4. intercepting or examining the content of messages, files, or communications without authorization;
2.3.5. infringing upon the copyright of computer programs, data compilations and all other works (literary, dramatic, artistic or musical);
2.3.6. infringing upon the legal protection provided by trademark law and the common law for names, marks, logos, and other representations that serve to distinguish the goods or services of one person from another;
2.3.7. making unauthorized copies of proprietary software, or offering unauthorized copies of proprietary software to others;
2.3.8. failing to maintain the confidentiality of passwords, access codes or identification numbers used to access UBC Electronic Information and Systems;
2.3.9. seeking information on passwords or information belonging to another User without authorization;
2.3.10. accessing or examining other accounts, files, programs, communications or information without authorization;
2.3.11. destroying, altering, dismantling, disfiguring or disabling UBC Electronic Information and Systems without authorization;
2.3.12. damaging or altering the hardware or physical components of UBC Systems without authorization;

2.3.13. attempting to circumvent security controls on UBC Electronic Information and Systems without authorization;
2.3.14. knowingly introducing a worm or virus; and
2.3.15. engaging in any uses that result in the loss of another User's information without authorization.

2.4. Nothing in paragraph 2.3 shall be construed as preventing or restricting duly authorized system administrators or other technical personnel from carrying out their duties.

3. Security of UBC Electronic Information and Systems

3.1. All Users must comply with the Information Security Standards established under this policy regarding the security of UBC Electronic Information and Systems.

3.2. The CIO is responsible for:

3.2.1. developing and issuing the Information Security Standards, which must be consistent with this policy;
3.2.2. publishing the Information Security Standards on the UBC Information Technology web site for access by all Users; and
3.2.3. reviewing the Information Security Standards on a bi-annual basis or at such other interval as the CIO determines.

3.3. A committee (the "Advisory Committee") will be established by the CIO and will consist of representatives from the Office of the University Counsel, Human Resources, Faculty Relations, and the units responsible for maintaining and/or operating significant UBC Electronic Information and Systems. The Advisory Committee will provide advice to the CIO on the development of and ongoing updates to the Information Security Standards and will also provide advice to the relevant Responsible Executive with respect to any disagreements referred to him or her pursuant to paragraph 3.6 of this policy. In developing the Information Security Standards, the Advisory Committee and the CIO must consider best practices, resource availability and implementation schedules.

3.4. Academic and administrative units that wish to deviate from the Information Security Standards are required to request the authorization of the CIO before proceeding.

3.5. Where the Information Security Standards do not address the reasonable requirements of a unit's use of and access to UBC Electronic Information or Systems, the CIO may authorize a variance or update the Information Security Standards as appropriate.

3.6. If a disagreement arises and cannot be resolved in a timely manner between the CIO and the head of an academic or administrative unit in respect of the requested deviation then either party may refer the disagreement to the relevant Responsible Executive, who will decide the matter. This Responsible Executive may consult with the Advisory Committee and/or the other Responsible Executive if he or she determines it would be appropriate to do so.

4. Use of Non-University Systems for University Business

4.1 To maintain the security of UBC Electronic Information, Users intending to conduct University Business using systems other than UBC Systems must do so in accordance with the Information Security Standards.

5. Privacy of Users

5.1. Since paragraph 2.2 of this policy authorizes the incidental personal use of UBC Electronic Information and Systems, the University recognizes that these resources may contain records relating to this personal use, e.g. personal emails, documents, voicemails, text messages, and records of internet and social media use (the "Personal Use Records").

5.2. While the University takes reasonable measures to back up information and protect it from loss, the University cannot guarantee that Personal Use Records will be retained in the UBC Systems or remain confidential. To protect their Personal Use Records from inadvertent access, disclosure or destruction, Users are encouraged to store them separately from UBC Electronic Information and back them up on a regular basis. Where Users intermingle Personal Use Records with UBC Electronic Information, they increase the risk that the University will unintentionally access the Personal Use Records in the course of accessing UBC Electronic Information for University Business purposes.

5.3. Users should understand that the University routinely monitors network transmission patterns such as source/destination, address/port, flags, packet size, packet rate, and other indicia of traffic on UBC Systems. University system administrators and other technical personnel also perform routine maintenance of UBC Systems. This routine monitoring and maintenance may unintentionally reveal Personal Use Records.

5.4 The University will not intentionally access, use or disclose Personal Use Records unless it has the consent of the User, or:

5.4.1. securing the User's consent would compromise (a) the health or safety of an individual or a group of people, (b) the availability or accuracy of the information, or (c) an investigation or a proceeding related to a breach of law or policy or the employment of the User;
5.4.2. such access has been authorized by the head of the relevant unit and the University Counsel, or their delegates, in accordance with the procedure set out in the Information Security Standards; and
5.4.3. the University is legally authorized to do so.

5.5 Notwithstanding anything in paragraph 5.4, the University will take such actions as are necessary to comply with any legal obligations.

5.6. Users should be aware that electronic information does not necessarily disappear after it has been deleted. The University may, in accordance with this policy, retrieve or reconstruct Personal Use Records generated, stored, or maintained on UBC Systems even after they have been deleted.

6. Administrative Responsibilities

6.1. Administrative heads of unit are responsible for establishing and maintaining UBC Electronic Information and Systems within their areas of responsibility. These responsibilities include:

6.1.1. ensuring that UBC Electronic Information and Systems are secured with adequate controls, with particular care concerning User identification and validation measures;
6.1.2. ensuring, as appropriate or required, that UBC Electronic Information within their area of responsibility is maintained, transmitted, and stored in a secure and consistent manner that adheres to all relevant University policies and standards;
6.1.3. authorizing access for individuals to UBC Electronic Information and Systems within their area of responsibility;
6.1.4. renewing, retiring, and revoking User authorizations within their area of responsibility;
6.1.5. ensuring that a contingency plan, including appropriate data back-up systems and recovery systems, is being used within their unit;

6.1.6. ensuring that breaches and potential breaches of this policy occurring within their unit are resolved and/or referred to the CIO, as appropriate, and that where they are so referred, continuing to assist in the investigation, preserving evidence where required;
6.1.7. ensuring that technical staff within their unit are aware of and adhere to this policy, and that they support University standards in the design, installation, maintenance, training, and use of UBC Electronic Information and Systems;
6.1.8. working with UBC Information Technology to make training and other information and resources necessary to support this policy available to Users in their unit; and
6.1.9. taking immediate and appropriate action when they become aware of violations of this policy or its procedures.

7. Definitions

7.1. *Academic Freedom* is defined in the UBC Vancouver and UBC Okanagan calendars.

7.2. *UBC Electronic Information* is electronic information needed to conduct University Business.

7.3. *UBC Electronic Information and Systems* includes UBC Electronic Information and UBC Systems.

7.4. *UBC Systems* are services, devices, and facilities that are owned, leased or provided by the University, and that are used to store, process or transmit electronic information. These include, but are not limited to:

7.4.1. computers and computer facilities;
7.4.2. computing hardware and equipment;
7.4.3. mobile computing devices such as laptop computers, smartphones, and tablet computers;
7.4.4. electronic storage media such as CDs, USB memory sticks, and portable hard drives;
7.4.5. communications gateways and networks;
7.4.6. email systems;
7.4.7. telephone and other voice systems; and
7.4.8. software.

7.5. *University Business* means activities in support of the administrative, academic, and research mandates of the University.

7.6. *Users* are faculty, staff, students, and any other individuals who use UBC Electronic Information and Systems.

Attachment 3: Summary of Responses to Call for Comments, Policy #104

Applicable Paragraph	Description of Comment	Committee Recommendations
Background & Purposes	The Policy should only apply to "administrative data". It should not apply to academic and research information because the University does not control or own such information.	This change is not recommended. The Committee strongly believes that all UBC Electronic Information stored on UBC Systems should be subject to the same acceptable use and security standards. This is essential to ensure the integrity and security of these resources. However, the Policy is not intended to erode academic freedom or regulate the "ownership" or "control" of academic and research information, which are determined by factors outside the scope of this Policy. To address the foregoing concerns, the Committee has made the following significant changes: • Inserted wording into the Background and Purposes section confirming that the policy will be interpreted in the context of the principle of academic freedom. • Inserted wording (paragraph.1.5) to emphasize that teaching materials and research information are exempt from the Freedom of Information and Protection of Privacy Act.
Background & Purposes	Insert a statement that UBC owns all UBC Electronic Information and Systems.	This change is not recommended. As discussed above, UBC does not necessarily own all of the information stored in its systems. The purpose of the Policy is simply to prescribe consistent use and security standards for all of this information, regardless of ownership.
Background & Purposes	Insert statement confirming adherence with any relevant legal requirements or collective agreements.	Agreed.
1.2.3	Revise to state "assisting in the investigation of breaches and potential breaches of the policy".	Agreed.

Attachment 3: Summary of Responses to Call for Comments, Policy #104

Applicable Paragraph	Description of Comment	Committee Recommendations
1.2.3	The CIO's involvement in investigations should not be mandatory; insert "as appropriate" into this sentence.	Agreed.
1.4	Insert statement confirming that application of this article should not have retroactive application.	No changes recommended, because policies generally do not have retroactive application.
1.4	Revise wording to state "Users who breach this policy may be subject to the full range of disciplinary actions up to and including termination of employment."	No changes recommended, because termination is implicitly part of the full range of disciplinary actions.
1.6	Add recognition that UBC Systems that are specifically designed for a purpose unrelated to the business of the University are exempted from the scope of this policy.	Agreed.
2.1.2	Add a reference to the Respectful Environment Statement.	Agreed.
2.2	The phrase "incidental personal use" is somewhat vague.	No changes recommended. Since there is a wide variety of UBC Systems, it is necessary to use general language.
2.2	The phrase "not an unacceptable use" contains a double negative.	Agreed. The term "unacceptable" has been changed to "prohibited".
2.3	The phrase "for their intended purpose" is somewhat vague.	No changes recommended. Since there is a wide variety of UBC Systems, it is necessary to use general language.

Attachment 3: Summary of Responses to Call for Comments, Policy #104

Applicable Paragraph	Description of Comment	Committee Recommendations
2.3	We are concerned with the fact that prohibited uses are limited to those that that disrupt or interfere with the use of the resources for their intended purpose. We think it should read that any use that is inconsistent with the intended purpose is an unacceptable use.	No changes recommended. The incidental personal use of UBC Electronic Information and Systems, which is specifically authorized by paragraph 2.2, may sometimes be inconsistent with the intended purpose of those systems. Such inconsistent use is acceptable provided that it does not disrupt or interfere with the intended purpose.
2.3	Several additional examples should be added, such as: "creating, transmitting, or viewing pornography or other sexually inappropriate, offensive, or explicit material"; "gambling"; "excessive use of social media such as Facebook, twitter, and YouTube"; "performing work for any business, company, proprietorship, or other entity (including the user's own business) other than the University"; "disclosing anyone's personal information contrary to privacy legislation."	No changes recommended. The Committee felt that some of these examples were too vague; others were already covered by other examples; and others might infringe upon academic freedom.
2.3.2, 2.3.6, 2.3.7	Remove these paragraphs. They are redundant because paragraph 2.3.1 already prohibits "breaching applicable laws or University policies".	No changes recommended. The Committee felt that it would be useful to include these specific examples of unacceptable uses.
2.3.4	This paragraph should state "intercepting or examining the content of messages, files, or communications not intended for the user".	This recommendation has been addressed by adding "without authorization".
2.3.8	Specify some kind of intentionality requirement with respect to this paragraph.	No changes recommended. This paragraphs describes an action (failing to maintain confidentiality of passwords) that is unacceptable even if unintentional.

Attachment 3: Summary of Responses to Call for Comments, Policy #104

Applicable Paragraph	Description of Comment	Committee Recommendations
2.3.10, 2.3.11, 2.3.15	Specify some kind of intentionality requirement with respect to these paragraphs.	This recommendation has been addressed by adding "without authorization".
2.4	It is unclear who is a "duly authorized system administrator or other technical personnel".	No changes recommended. Managing access to Electronic Information and Systems is the responsibility of administrative heads of unit (see paragraph 6.1). They will define the duties of administrators and other technical personnel with respect to their systems.
3.1	Requiring users of UBC systems (including the general public and other primarily non-technical users) to comply with the UBC Information Security Manual may be challenging as it is quite technical in nature. We suggest the Information Security Standards be revised so each type of user better understands what they are required to comply with.	Agreed. The Information Security Standards, which are being gradually released over the coming months, will be separate from the Information Security Manual. The Standards are intended to be concise and to use simple, direct language suitable for their target audience.
3.2.1	Amend this paragraph to reflect appropriate limitations: "… developing and issuing the Information Security Standards, which must be consistent with this policy and in accordance with the applicable statutory and common law and any collective agreement of which the University is a party to."	The recommendation has been addressed by a new paragraph in the Background and Purposes section that affirms that the Policy should be interpreted in accordance with all legal requirements.
3.3	Given the potential for breaches/discipline, representatives from Human Resources/Faculty Relations should be included on the Advisory Committee.	Agreed.

Attachment 3: Summary of Responses to Call for Comments, Policy #104

Applicable Paragraph	Description of Comment	Committee Recommendations
3.6	The policy should state the process of policy exemptions, deviations and disagreement resolutions will be transparent and timely.	Agreed in part. The paragraph has been amended by adding the requirement to resolve the matter "in a timely manner".
4.1	The meaning of "University business" is unclear.	Agreed. A definition has been added to section 7.
4.1	Does this paragraph prohibit the use of personal smartphones, tablets and computers for University Business purposes? How about the use of computers owned by Health Authorities or non-UBC Institutes?	This paragraph was not intended to prohibit the use of personal devices, or devices owned by other organizations, as long as they are secure. The Committee has rewritten this paragraph to clarify that non-UBC systems may be used to conduct University Business, provided that these systems comply with the Information Security Standards. The CIO has already created an Information Security Standard on Mobile Access to Services and Data. Since the vast majority of personally owned devices are already compliant with this Standard, this requirement should not have a significant impact.
5.1	Insert statement affirming commitment to personal privacy and to the applicable laws and collective agreements.	The recommendation has been addressed by a new paragraph in the Background and Purposes section that affirms that the Policy should be interpreted in accordance with all legal requirements, including collective agreements.
5.1	This paragraph should be changed to state "... e.g. personal emails, documents, text messages, internet use and activity (including social media use and activity), website logs, and voicemails (the "Personal Use Records").	Agreed. The paragraph has been amended (using slightly different wording).
5.2	Use a plain language alternative to "does not warrant".	Agreed. Replaced "does not warrant" with "cannot guarantee".

Attachment 3: Summary of Responses to Call for Comments, Policy #104

Applicable Paragraph	Description of Comment	Committee Recommendations
5.2	This paragraph should be changed to state "… protect it from loss, the University does not have custody and control over the Personal Use Records and as such cannot warrant their retention on UBC Systems."	The committee did not recommend using the terms "custody or control", the meaning of which may vary depending on the context. However, the Committee did add a sentence to this paragraph emphasizing that Personal Use Records should not be intermingled with UBC Electronic Information.
5.3	The word "inadvertently" should be deleted.	Agreed. Replaced "inadvertently" with "unintentionally".
5.3	We recommend defining routine monitoring and any notification when it occurs.	Network transmission patterns and other indicia of traffic are monitored to ensure the security and integrity of the network. Monitoring procedures and tools are constantly evolving, so it is not practicable to define this monitoring more precisely in this Policy.
5.4	We recommend the University first obtain informed consent and alternatively only access the Personal Use Records if in accordance with the relevant law and collective agreements.	Agreed. Paragraph 5.4 has been amended to clarify the circumstances under which UBC is authorized to intentionally access Personal Use Records.
5.4	This paragraph be changed to state "Users should understand that they have no expectation of privacy with respect to their use of UBC Electronic Information and Systems, including Personal Use Records. While the University does not, as a routine matter, review Personal Use Records generated, transmitted, stored, or maintained on UBC Systems, the University retains the right to monitor, inspect, review and retain the Personal Use Records for legitimate University purposes without further notice to the User."	Users of UBC Systems do have a limited expectation of privacy when they are personally using these systems. Therefore, UBC cannot assert an unfettered right of access to Personal Use Records. The proposed wording of section 5.4 balances the privacy rights of the systems against the legitimate requirements of the University to review the records on these systems under some circumstances.

Attachment 3: Summary of Responses to Call for Comments, Policy #104

Applicable Paragraph	Description of Comment	Committee Recommendations
5.4	This paragraph should contain a clear reference to UBC's obligation to respond to freedom of information requests under the Freedom of Information and Protection of Privacy Act.	This change is not necessary because paragraph 5.4 has been amended to authorize UBC to access Personal Use Records where it is required to do so by law.
6.1	Strict interpretation of the policy and its related Information Security Standards may involve significant new transition or implementation costs. UBC should acknowledge these effects, and provide free, timely guidance, resources and support to affected units to address and mitigate such effects.	Most of the requirements listed in this paragraph already apply to administrative systems under the current policy. The new policy merely ensures consistency by stipulating that UBC systems used for academic and research purposes are subject to the same requirements. It is unlikely that this will involve significant new costs. The CIO will make efforts to facilitate the transition.
6.1.6	Para 6.1.6 should state: "ensuring that breaches and potential breaches of this policy... continuing to assist in the investigation including preserving evidence"	Agreed.
7.4.3	Add "PDAs" to examples of mobile computing devices.	This change is not recommended, as "PDA" is not a commonly used term.
7.8	Insert "post doctoral fellows" into definition.	This change is not recommended, as post doctoral fellows fall under the catch-all phrase "all other individuals".

Attachment 4: Draft List of Systems Exempted from Policy #104

Procedure Name	Exemptions from Policy #104
Date	2013-05-10
Approval Date	

Executive Summary

Paragraph 1.6 of Policy #104, Acceptable Use and Security of UBC Electronic Information and Systems, provides that:

> **1.6 Where a UBC System is not intended to be used for University Business, the CIO must, in consultation with the Office of the University Counsel, approve separate terms of use that govern the use of such system. Upon such approval, this policy will not apply to such system.**

This Directive contains a list of the systems that are exempted from Policy #104 under the above paragraph.

Dependencies

Policy #104

Directives

The Chief Information Officer, in consultation with the Office of the University Counsel, has approved separate terms of use that govern the use of the following systems:

Exempted System	Terms of Use
Visitor Wireless Network	Appropriate Use Policy
ResNet Service	Service Agreement, Appropriate Use Policy
Student & Alumni E-mail Service	Terms of Service

Author

Paul Hobson, Director of Enterprise Architecture, UBC IT

Reviewers

Paul Hancock, Access and Privacy Manager, Office of the University Counsel

Review Date

May 13, 2013

Attachment 5: Draft Information Security Standards

INFORMATION SECURITY STANDARD

Requesting Variances from Information Security Standards

Introduction

1. In order to protect University information assets, the Chief Information Officer (CIO) has issued binding Information Security Standards. Academic and administrative units that wish to deviate from these Information Security Standards are required to request a variance from the CIO. This document establishes the procedure for requesting such a variance.

2. This document has been issued by the Chief Information Officer under the authority of Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems. Questions may be referred to information.security@ubc.ca.

Definitions

3. *Advisory Committee* means the Information Security Governance Committee, which consists of representatives from the Office of the University Counsel, Human Resources, Faculty Relations, and the units responsible for maintaining and/or operating significant UBC Electronic Information and Systems.

4. *Chief Information Officer* means the Chief Information Officer in the UBC Information Technology Department, or his duly authorized delegate.

5. *Responsible Executive* means the Vice-President, Academic and Provost (for UBC Vancouver) and the Deputy Vice-Chancellor (for UBC Okanagan).

6. *Requester* means the administrative head of unit requesting the deviation in the Information Security Standard.

Variance Request Procedure

Initial Request

7. The Requester must submit the following information to information.security@ubc.ca:

    a. contact information,
    b. description of the requested variance and expected duration,
    c. explanation of why the variance is warranted,
    d. analysis of risk associated with granting the variance, and what controls will be in place to manage this risk, and
    e. analysis of cost and resource implications of granting the variance.

8. When considering the request for a variance, the CIO may seek the input of the Advisory Committee if he or she considers this appropriate.

9. The CIO may authorize a variance from the Information Security Standards in any of the following circumstances:

    a. the Requester is temporarily unable to meet the compliance standard,
    b. compliance is not achievable for technical or financial reasons,
    c. an alternate method of compliance is available that offers equivalent or better security, or
    d. the variance is otherwise reasonable and is consistent with the Information Security Standards.

10. If the CIO approves a deviation, he or she will set out the terms of the variance, including any applicable mitigation requirements or other conditions.

11. If the CIO denies the requested deviation, he or she will provide an explanation and, if possible, a suggestion of alternatives.

Resolution of Disagreements

12. If a disagreement arises and cannot be resolved in a timely manner between the CIO and the Requester in respect of the requested deviation then either party may refer the disagreement to the relevant Responsible Executive, who will decide the matter. This Responsible Executive may consult with the Advisory Committee and/or the other Responsible Executive if he or she determines it would be appropriate to do so.

13. The Responsible Executive's decision is final.

INFORMATION SECURITY STANDARD

Accessing Electronic Accounts and Records

Introduction

1. This Information Security Standard establishes a procedure for University staff and faculty members to gain access to electronic accounts and records on UBC Systems, such as email accounts, Student Information System accounts, voicemail accounts, internet usage records, and telephone logs.

2. This document has been issued by the Chief Information Officer under the authority of Policy #104, Acceptable Use and Security of UBC Electronic Information and Systems. Questions may be referred to information.security@ubc.ca.

Definitions

3. *Personal Use Records* are records relating to Users' personal use of UBC Systems, e.g. personal emails, documents, voicemails, text messages, and records of internet and social media use.

4. *UBC Electronic Information* is electronic information needed to conduct University Business.

5. *UBC Systems* are services, devices, and facilities that are owned, leased or provided by the University, and that are used to store, process or transmit electronic information. These include, but are not limited to:

    a. computers and computer facilities;
    b. computing hardware and equipment;
    c. mobile computing devices such as laptop computers, smartphones, and tablet computers;
    d. electronic storage media such as CDs, USB memory sticks, and portable hard drives;
    e. communications gateways and networks;
    f. email systems;
    g. telephone and other voice systems; and
    h. software.

6. *University Business* means activities in support of the administrative, academic, and research mandates of the University.

7. *Users* are faculty, staff, students, and any other individuals who use UBC Electronic Information and UBC Systems.

Access with Consent

8. Policy #104 authorizes reasonable personal use of UBC Systems. For privacy reasons, it is preferable to get the consent of Users before accessing electronic accounts and records.

9. Consent must be in writing, but does not need to be signed (an email is acceptable). You may use the attached Form of Consent or equivalent language.

10. If you have secured the consent of the User, you do not require the authorization of the Head of Unit or the Office of the University Counsel to access the account or records in question.

Access without Consent

General Principles

11. It is occasionally necessary to gain access to an electronic account or record without the User's consent. To ensure that the University's business requirements are balanced against the User's privacy interests, access without consent requires the authorization of the head of unit and the Office of the University Counsel. This authorization will depend on the type of information you are intending to access and what you are planning to do with this information after you access it.

Criteria for Access to UBC Electronic Information without Consent

12. If you only need to view UBC Electronic Information, then the head of unit and the Office of the University Counsel will authorize you to access the electronic accounts/records provided that:

    a. you have a pressing reason to view this information for University Business purposes, and
    b. you have not been able to secure the consent of the User despite making reasonable attempts to do so, e.g. the User is incapacitated, has gone on vacation without leaving contact information, or has been terminated and is unwilling or unavailable to provide consent.

Example:

An employee has been incapacitated in a motor vehicle accident. Her supervisor needs to access the employee's work email account to check for any time-sensitive work-related messages, but the employee is unable to consent to this access. Under these circumstances, access would normally be authorized. The supervisor should not read the employee's personal messages, however.

13. When accessing accounts or records to view UBC Electronic Information, you must make reasonable efforts to avoid viewing the User's Personal use Records. If you inadvertently view Personal Use Records, you must not copy, alter, delete, use or disclose these records unless they provide evidence that the User has violated Policy #104, in which case you must consult with the Office of the University Counsel to determine the appropriate action.

14. In addition to Personal Use Records, accounts may also contain other sensitive information, such as teaching materials or research information. You must respect the confidentiality of this information as its unauthorized use and disclosure may harm the interests of the User and the University as a whole.

Criteria for Access to Personal Use Records without Consent

15. If you need to view Personal Use Records, then the head of unit and the Office of the University Counsel will only authorize you to access the electronic accounts/records if the University is legally required to do so, or if securing consent would compromise:

    a. the health or safety of an individual or a group of people,
    b. the availability or accuracy of the information, or
    c. an investigation or a proceeding related to a breach of law or policy or the employment of the User.

Procedure for Access

16. If you intend to access accounts and records, you must complete the Access Form and submit it to the administrator who controls access to the account. If you do not have the User's consent, you must also request the head of unit and the Office of the University Counsel to sign the form to authorize access. The administrator will grant access to the account/records only for the period of time specified in the access form.

Form of Consent for Access to Accounts/Records

I, [NAME], authorize UBC to access [ACCOUNTS/RECORDS] for the following purpose: [DESCRIBE PURPOSE]. This authorization is effective until [DATE].

Request to Access Electronic Accounts & Records

INFORMATION ABOUT REQUEST FOR ACCESS			
UBC IT trouble ticket number		Date of request	
Name	Department	Email	Phone

ACCOUNT/RECORDS TO BE ACCESSED
Computer account – username
Communications account – phone number
Other account or records – please specify

USER (ACCOUNT/RECORD HOLDER)		
Name	Department	
Student ID	Employee ID	Contact phone number

ACCESS DETAILS

Type(s) of information that you intend to access

- ☐ UBC Electronic Information (electronic information needed to conduct University business)
- ☐ Personal Use Records (records relating to the personal use of the account/records by the User)

Who will have access to the account/records

How long access is required

What will be done to avoid unauthorized access to and disclosure of personal information stored in the account/records

What should be done to the account/records when access is no longer required

- ☐ Return to User
- ☐ Archive data and delete account
- ☐ Other (specify):

AUTHORITY FOR ACCESS
Select one of the following authorities for accessing the account/records: ☐ The User has consented, in writing, to the access (attach consent) ☐ You do not have the User's consent, but the University is legally required to access the account/records ☐ You do not have the User's consent, but • you have a pressing reason to view UBC Electronic Information (no Personal Use Records will be viewed), and • you have not been able to secure the User's consent despite making reasonable efforts to do so. ☐ You do not have the User's consent, but • you wish to view Personal Use Records, and • securing the User's consent would compromise (a) the health or safety of an individual or a group of people, (b) the availability or accuracy of the information, or (c) an investigation or a proceeding related to a breach of law or policy or the employment of the account/record holder
If you do not have consent, provide detailed reasons for accessing the account/records

Head of Unit approval of access without consent	Name/Position	Signature
	Conditions/Restrictions	Date
University Counsel approval of access without consent	Name/Position	Signature
	Conditions/Restrictions	Date

TO BE COMPLETED BY UBC IT OR ACCOUNT ADMINISTRATOR		
Access granted to		
Date/time access approved	Name/Position	Signature
Date/time access granted	Name/Position	Signature
Date/time access revoked	Name/Position	Signature
Notes		

For University Counsel's review, forward to Access & Privacy Manager:

- *By PDF: access.and.privacy@ubc.ca*
- *By fax: 604.822.8731*

After approval, forward to:

Voice Services (phone record related requests): • *By PDF: http://web.it.ubc.ca/forms/isf/* • *By fax: 604.822.5520*	*Responsible Use Administrator (computer account related requests):* • *By PDF: security@ubc.ca* • *By fax: 604.822.5116*

INFORMATION SECURITY STANDARD

Mobile Access to Services and Data

Introduction

1. This Information Security Standard establishes requirements for all Mobile Devices that are used to store or gain access to Personal Information, whether these devices are personally owned or supplied by the University. In keeping with the University's open computing environment, the University does not place any restrictions on device type, so long as the device complies with these requirements.

2. This document has been issued by the Chief Information Officer under the authority of Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems. Questions may be referred to information.security@ubc.ca.

Definitions

3. *Mobile Devices* are any portable computing or data storage devices. These include:

    a. Laptops (a mobile computer small enough to fit on a user's lap),
    b. Mobile Computing Devices (computing devices smaller than laptops, such as smartphones, tablet computers and PDAs), and
    c. Mobile Storage Devices/ Media (portable devices used to store electronic information , such as USB sticks, portable drives, memory cards, CDs, DVDs)

4. *Personal Information* is recorded information about an identifiable individual, with the exception of the names and business contact information of employees, volunteers and service providers.

Alternatives to Storage of Personal Information

5. As Mobile Devices are vulnerable to loss or theft, you should avoid storing Personal Information on these devices. Instead of downloading Personal Information, it is preferable to use your device to access the information remotely at the campus datacentre. There are two ways to do this:

    a. The preferred method is to use a Virtual Desktop Interface (VDI) and keep all information that you work with inside the VDI session. VDI is a service available through UBC IT, which creates a "virtual" computer that can be accessed from home computers, laptops, desktops, tablets and even smartphones; the information remains securely in a UBC datacentre.
    b. Alternatively, you can use a Virtual Private Network (VPN) interface to access the information on a server located in a secure datacentre on campus.

Requirements for Storage of Personal Information

6. As noted above, storage of Personal Information on Mobile Devices is not recommended. However, there may be situations where this is appropriate or necessary. For example, USB sticks are commonly used to transport large amounts of information. Also, if you are using a Mobile Device to access email, these emails (including emails containing Personal Information) may be backed up automatically on your device.

7. If it is necessary to store Personal Information on your Mobile Device, you must comply with the following requirements:

a. The device must be encrypted (unless it is a Laptop, in which case encryption is recommended but not required). Encryption must comply with the UBC encryption standards as described in the Information Security Standard on Encryption Requirements.
b. If the device offers a remote data destruction feature for use in event of theft, you must enable this feature.
c. Before disposing of the device or transferring it to another user, you must ensure that all data is permanently and irreversibly deleted. Deleting files is insufficient to prevent recovery of data.
d. You must delete and/or return any University-owned information stored on the device to the University upon request.
e. In the event that the device is lost or stolen, you must refer to the University's data loss procedure, which is set out in the Information Security Standards, and follow the required steps without delay. Be aware that even if a lost device is recovered, you must still follow the data loss procedure because the data on it may have been copied by someone else.

Additional Requirements for Laptops and Mobile Computing Devices

8. Laptops and Mobile Computing Devices (but not Mobile Storage Devices) have additional security features to help prevent a thief from getting access to the device. If you use such devices to store and/or gain access to Personal Information, you must also comply with the following requirements:

    a. Configure the device to require a password for use. This password must be at least five characters long. Also, many devices allow for data to be automatically erased if someone enters 10 consecutive incorrect passwords. Enable this feature if it exists.
    b. Enable the feature that locks your device automatically after a maximum of 30 minutes of activity. A shorter period of 5 minutes is recommended.
    c. If the device supports it, install and use up-to-date anti-virus software.
    d. Many devices include a feature that uses your device's GPS to locate the device in the event of loss. Enable this feature if your device supports it.

INFORMATION SECURITY STANDARD

Encryption Requirements

Introduction

1. This Information Security Standard explains when devices or files must be encrypted to safeguard their contents.

2. This document has been issued by the Chief Information Officer under the authority of Policy #104, Acceptable Use and Security of UBC Electronic Information and Systems. Questions may be referred to information.security@ubc.ca.

Definitions

3. *Personal Information* is recorded information about an identifiable individual, with the exception of the names and business contact information of employees, volunteers and service providers.

What is Encryption?

Overview

4. Encryption is the process of making information unreadable, to protect it from unauthorized access. After information has been encrypted, you need a secret key, or password, to unencrypt it and make it readable again. UBC's minimum standard for encryption is AES-128 bit encryption or equivalent; AES-256 bit encryption is recommended.

Is ZIP the same as encryption?

5. A ZIP file is not the same as encryption; it is simply a compressed file containing one or more files in an easy-to-transport package. Most ZIP programs contain the ability to protect the compressed file with strong encryption, but this is feature not turned on by default.

Is password protection the same as encryption?

6. Encryption uses passwords, but "encryption" and "password protection" are not the same. Encryption protects information by "scrambling" it to make it unreadable. Nobody can unencrypt the information unless they know the encryption password. By contrast, password protection does not make information unreadable, it merely creates a barrier that restricts access to the information. People may be able to find ways to bypass this barrier to get access to the information.

7. To illustrate the difference between password protection and encryption, and to show why encryption is a much more secure method of protecting information, imagine you are trying to protect a warehouse full of treasure. Locking the door with a key is analogous to password protection: as long as everyone uses the door, then the key is an effective way to protect the treasure; however, the lock would not prevent a thief from entering the warehouse through a window.

8. Now let's look at encryption. Imagine you have a special key that not only locks the warehouse door, but also camouflages the treasure so that nobody can find it. The only way to make the treasure return to normal is to unlock the door using the same key. With this type of security, a thief would never find the treasure, even if he managed to enter the warehouse through a window. No matter what the thief tried, he could not get the treasure unless he had the key.

When Encryption is Required

9. British Columbia's *Freedom of Information and Protection of Privacy Act* (FIPPA) requires the University to protect Personal Information. Encryption is a tool that we can use to comply with this legal requirement.

10. UBC's encryption requirements are explained below. Encryption may be required on a device level or a file level.

Device-Level Encryption Requirements

11. You are required to encrypt many computing or storage devices if you are storing Personal Information on them. The following is a summary of device-level encryption requirements:

Device	Encryption Requirement	Encryption Toolset
File servers located in datacentres	Encryption is not necessary.	n/a
File servers not located in datacentres	If possible, move the file server to a datacentre. Otherwise, Full Disk Encryption is recommended.	UBC IT central Encryption Service
Desktop computers	Full Disk Encryption is recommended.	UBC IT central Encryption Service
Laptop computers	Full Disk Encryption is recommended. Additional security requirements are set out in the Information Security Standard on Mobile Access to Services and Data.	UBC IT central Encryption Service
Mobile computing devices (e.g. smartphones, tablet computers)	Device-level encryption is required. Additional security requirements are set out in the Information Security Standard on Mobile Access to Services and Data.	Refer to owner's manual for instructions on activating encryption
Mobile storage devices/ media (e.g. USB sticks, CDs, DVDs)	Device-/media-level encryption is required. Additional security requirements are set out in the Information Security Standard on Mobile Access to Services and Data.	"How to Encrypt USB Sticks and Other Removable Media" guide

File-Level Encryption Requirements

12. When it is not feasible to apply encryption controls to mobile computing devices and portable storage devices at the device level, then you will need to encrypt any files stored on these devices that may contain Personal Information.

13. Encryption is also required at a file level when emailing large volumes of Personal Information. In this case, the approved method is to place the information in an encrypted file that you then attach to your email.

14. For instructions on encrypting Word, Excel and other general files, see our "How to Encrypt Files Using Common Applications" guide.

Password Requirements

15. Strong passwords must be used for encrypted files. Passwords must not contain all or part of the user's name, nickname, account name, address, date of birth, or any term that could easily be guessed by someone who is familiar with that person.

Information Technology

How to Encrypt Files Using Common Applications V1.1

Contents

Introduction

Encryption of Personal Information (PI) at UBC should be done using strong encryption, specifically AES-256 bit or equivalent; however, in order for the encryption to be strong, it must also have a strong password or passphrase. The reason for this is that if the encryption is strong then the easiest method of breaking the encryption is to "crack" the password. Short and simple passwords are easy to break while strong ones can takes years to crack.

Strong Passwords or Passphrases

A strong password in one which consists of a minimum of an 8 characters composed with Upper Case letters, Lower Case letters, Numbers and Symbols. E.g. "Irmb@7am" Alternatively a minimum 16 character passphrase is another option and should be something easily remembered and never shared – a nonsensical passphrase is best. e.g. "Pen eats 1 pizza!" For more details please refer to the "***Recommended Guidelines on Creating Secure Passwords***" in the UBC Information Security Manual.

If the purpose of this file encryption is to share PI files with others, then a password should be chosen that is not the same as your CWL or other UBC account passwords (email, file shares, intranet, etc.).

Safely Delivering the Encryption Password to the Recipient

When using these tools to encrypt and then share the information with colleagues, they will also need the password or passphrase; do not send them the password via e-mail, consider using the telephone, snail mail or sharing them during a meeting, etc. If the individual is receiving encrypted files on a regular basis, agree that all encrypted documents for a predetermined time will use the same password. It is recommended that the password be changed quarterly. If the file is encrypted in a shared workspace you may want to set a common password for all files in the folder requiring encryption.

Summary of Applications

The following How-To sections show how to use common applications, which can be used to help reduce the risk of exposure of PI through the proper use of file encryption.

Common application to assist in the encryption of PI for both storage and transmission:

Product	Version	Purpose
Microsoft Office	2007 or newer	Encrypt Word, Excel and other Microsoft Office files containing PI for e-mail or storage
7-Zip	9.20	Compress and encrypt files that you attach to email
AES Crypt	3.08	Encrypt files that you attach to email
WinZip	9 or newer	Compress and encrypt files that you attach to email
WinZip Courier	3.5	Compress and encrypt files that you attach to email

Full specifications for these encryption tools can be found in Appendix A.

Google Docs, OpenOffice and Other Applications

Google Docs, Office 365 and other similar "online" document services, typically store the information outside of Canada in foreign owned cloud-based servers. Legally, PI must be stored in Canada as a requirement of FIPPA; therefore, online applications like Google Docs and Office 365 must not be used with PI.

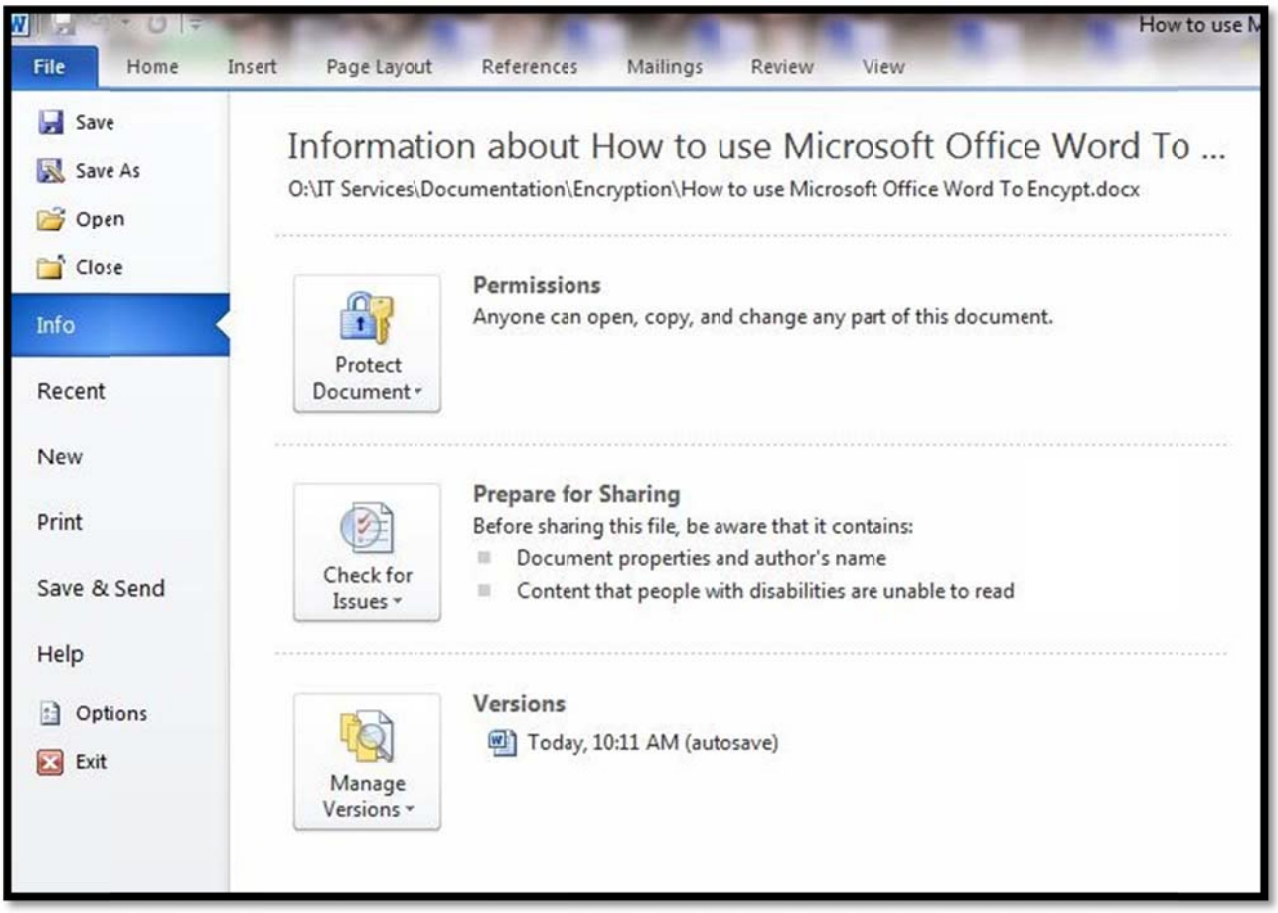
OpenOffice, LibreOffice and other applications that are installed on an individual's desktop/laptop computer **may** provide acceptable encryption; however, these applications have not been assessed for the strength of their security in protecting PI at UBC. Currently, the majority of employees at UBC use Microsoft Office and since the University has licensed it for all employees (regardless of whether they use Mac or Windows based systems), this document only focuses on encryption with MS Office.

1. How to Encrypt files using Microsoft Office 2007 or newer

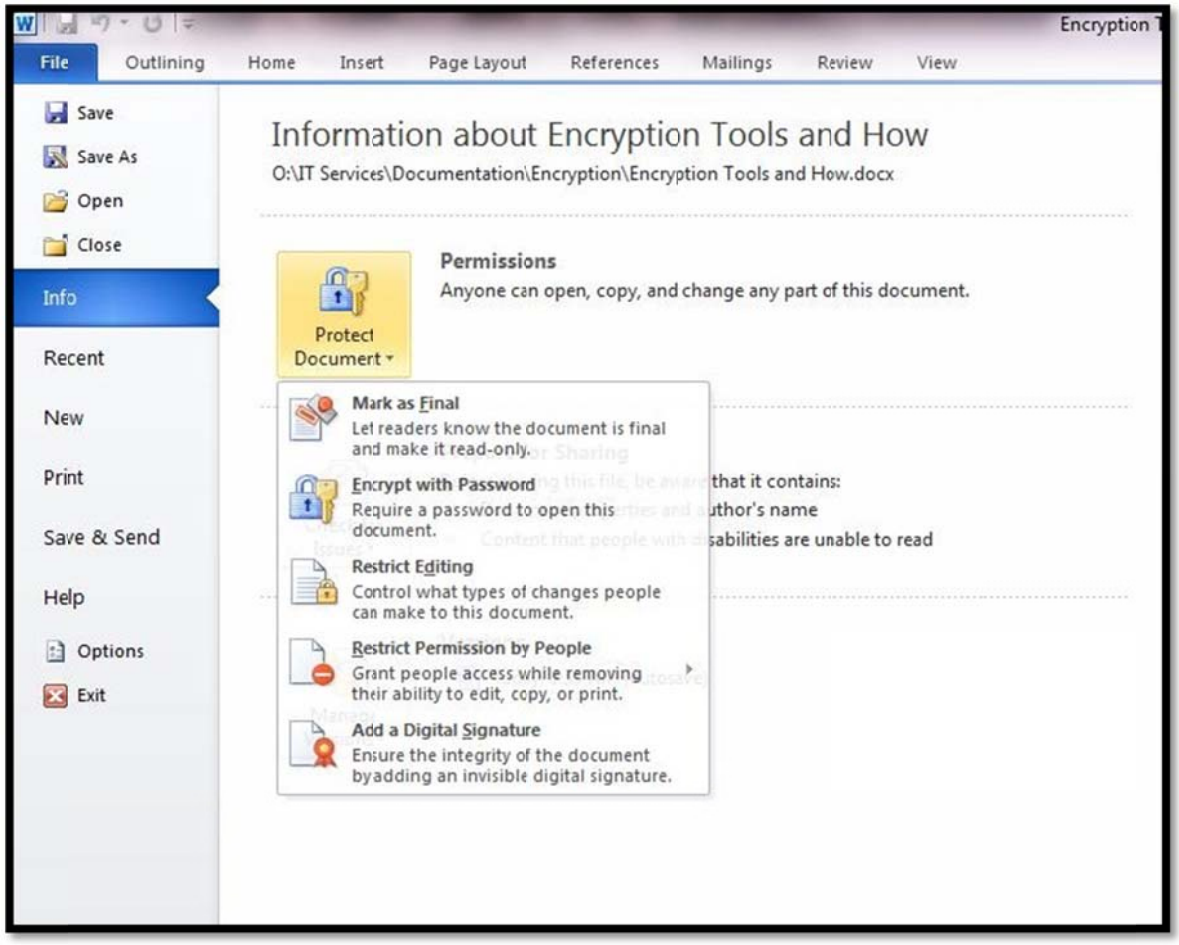
Microsoft Word, Excel, and PowerPoint 2007 (or newer) encrypts information using a "Protect" function; this function does not simply password protect a file but **fully encrypts** it using AES encryption.

Microsoft Word

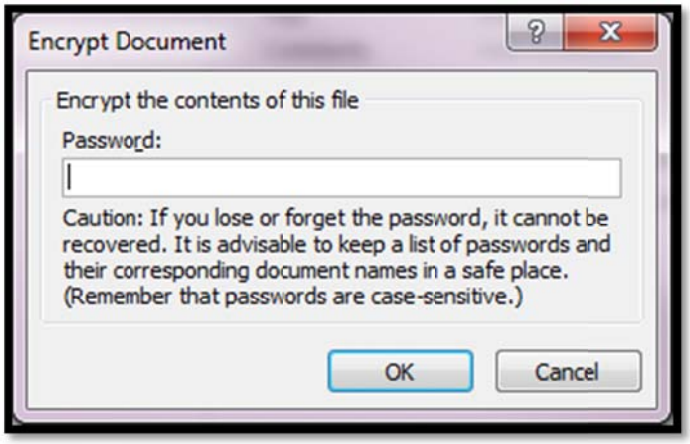
1.1. With your document open select the "File" tab.

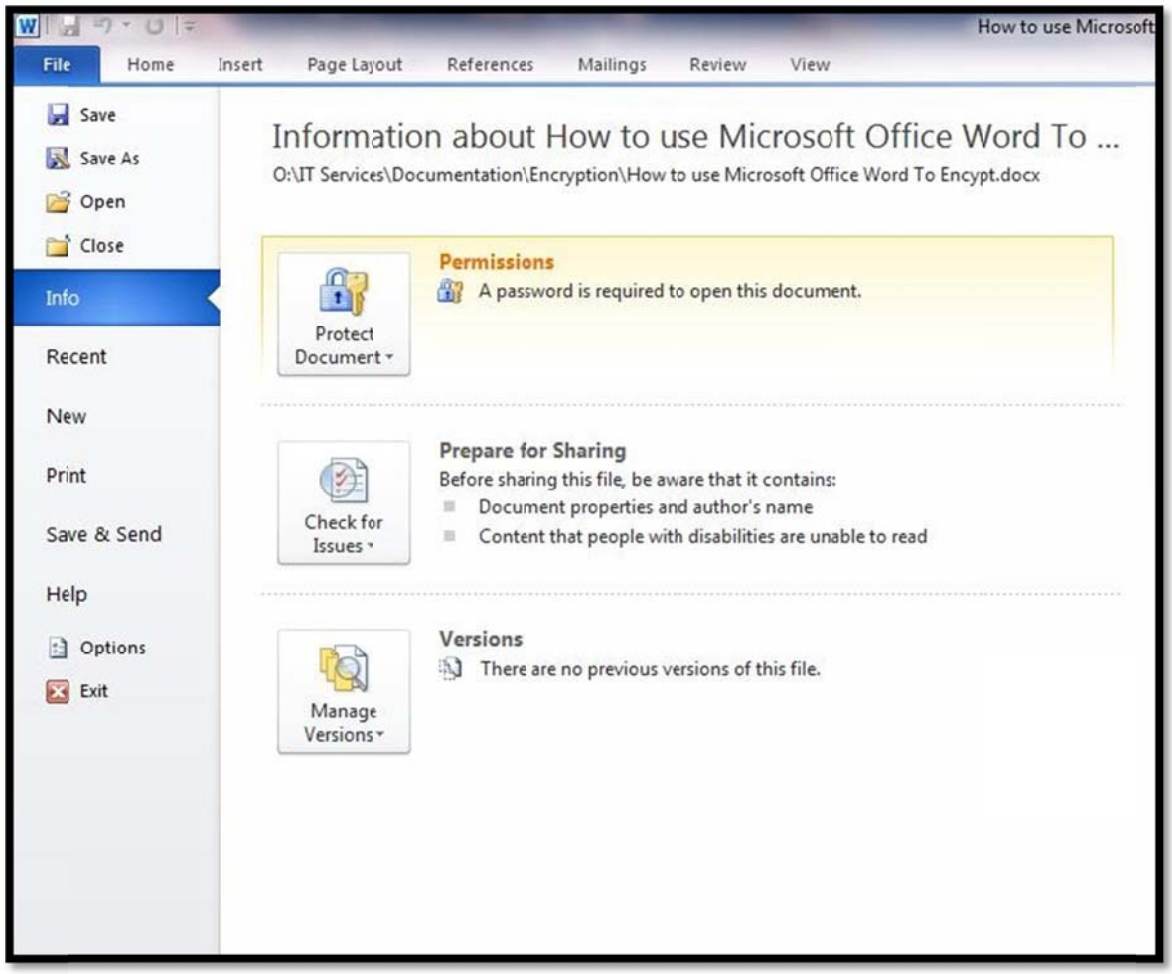


1.2. Click “Info” then select the “Protect Document” button with the downward pointing arrow.



1.3. Select the “Encrypt with Password” entry from the dropdown list, which will then prompt you for a password. It is recommended to use a strong password or passphrase.

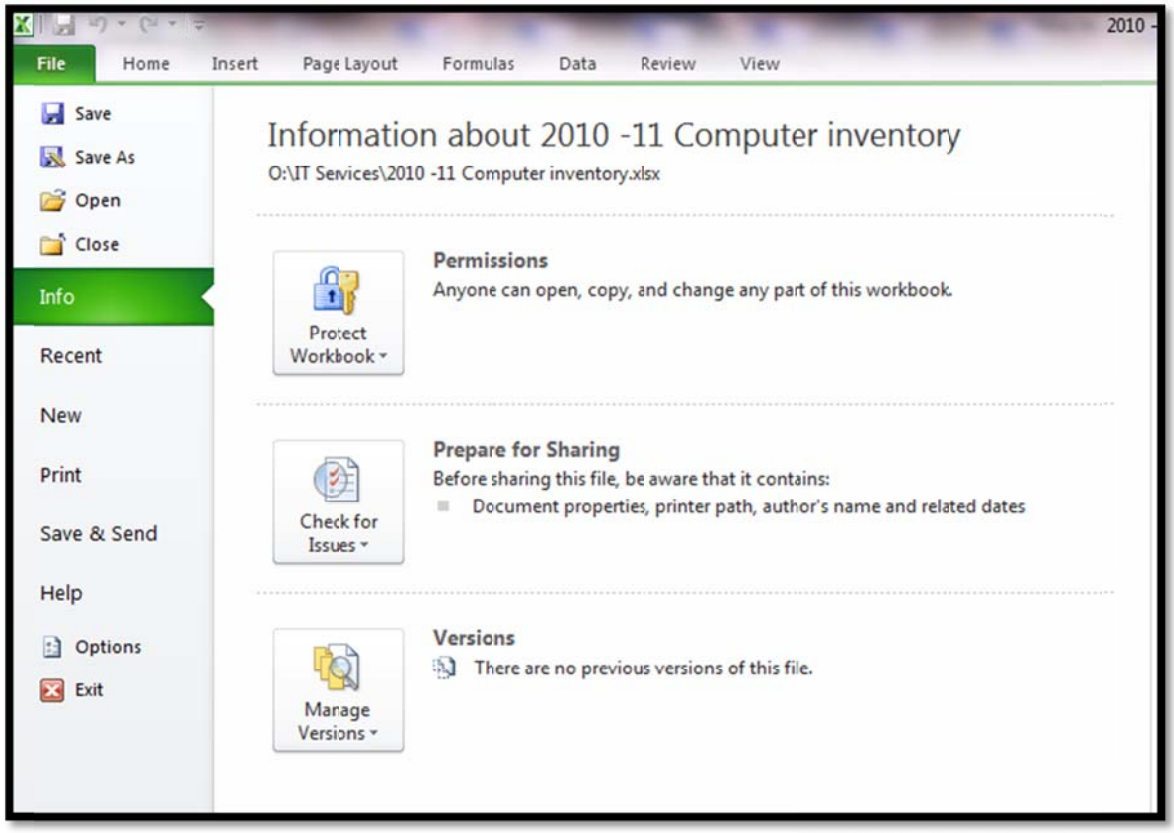




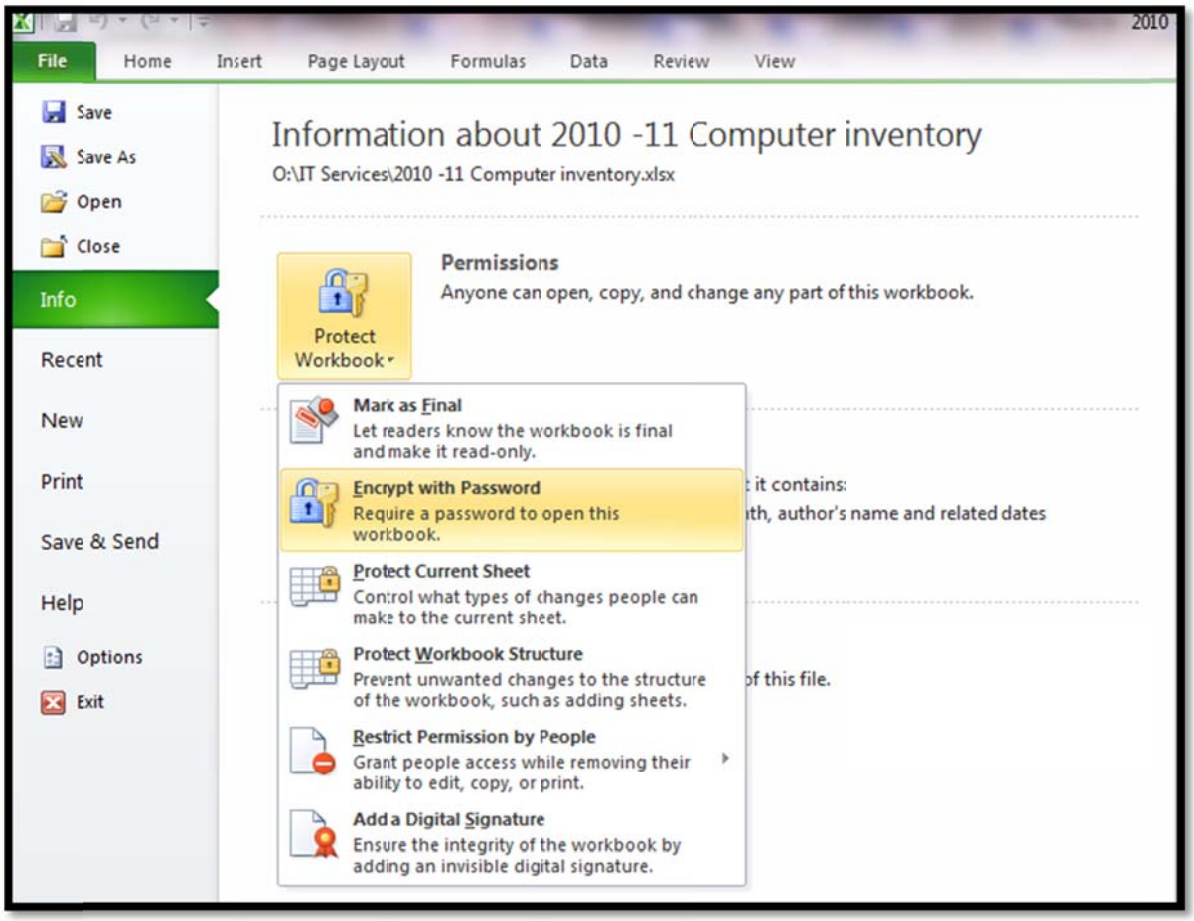
1.4. Once the file is encrypted, the password will be required to open the file.

1.5. To decrypt the file, follow the above steps and when prompted for the password, remove the password and save the file to secure network location or encrypted device. The file can now be opened without providing a password.

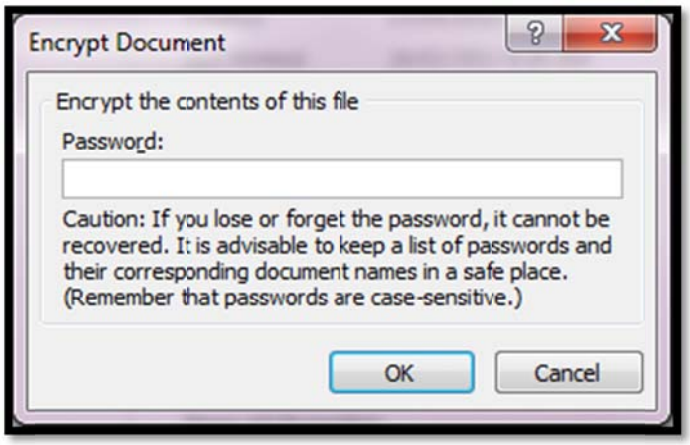
1.6. With a spreadsheet open, select the “File” tab.

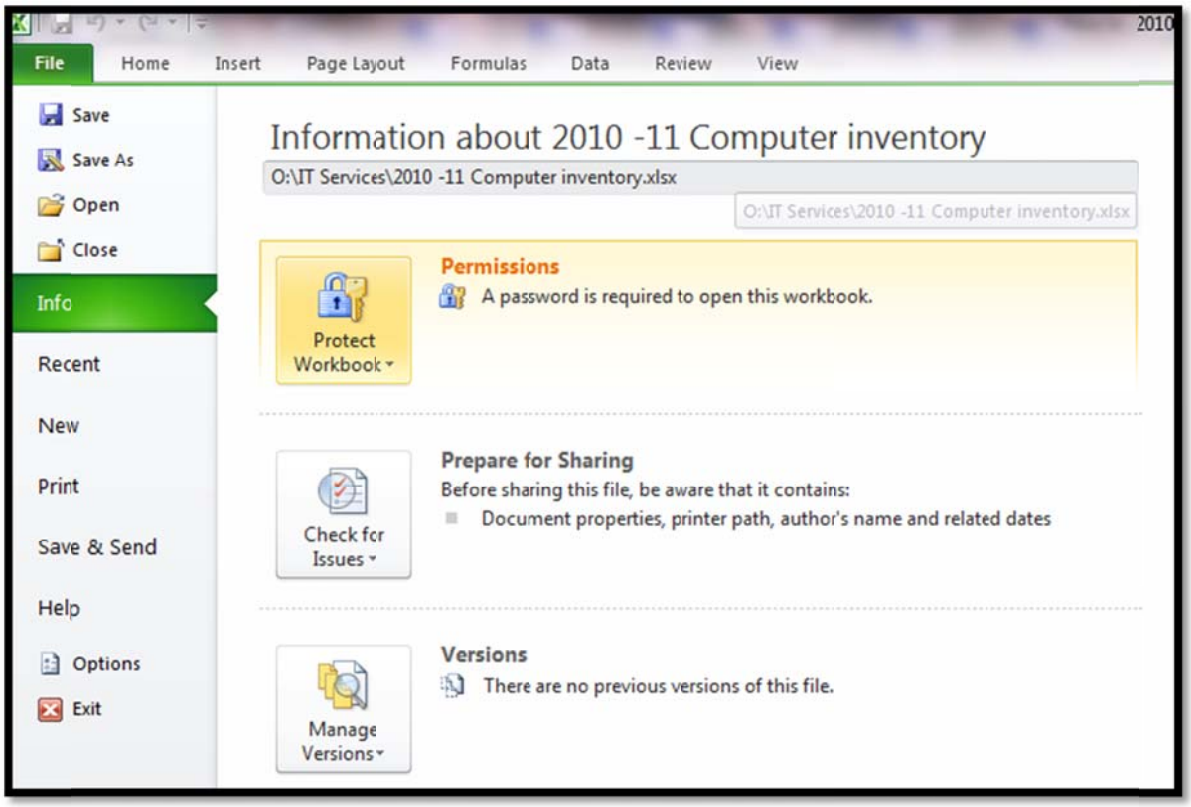


1.7. Click “Info” then select the “Protect Document” button with the downward pointing arrow.



1.8. Select the “Encrypt with Password” entry from the dropdown list, which will then prompt you to enter a password. It is recommended to use a strong password or passphrase.





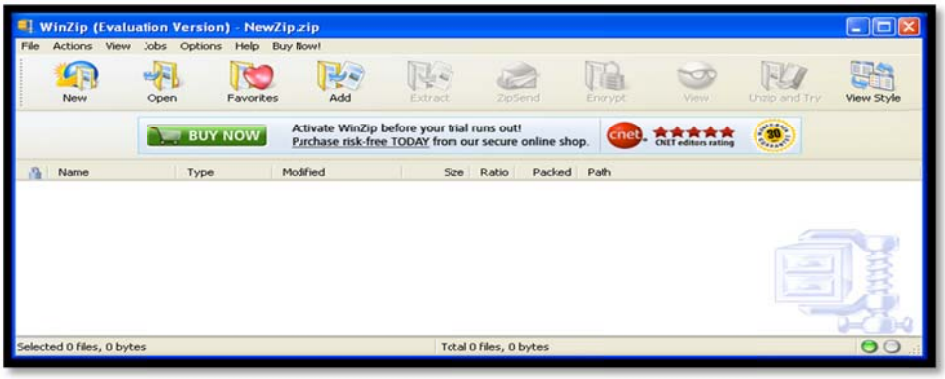
1.9. Once the file is encrypted, the password will be required to open the file.

2. How to use WinZip to Encrypt Files

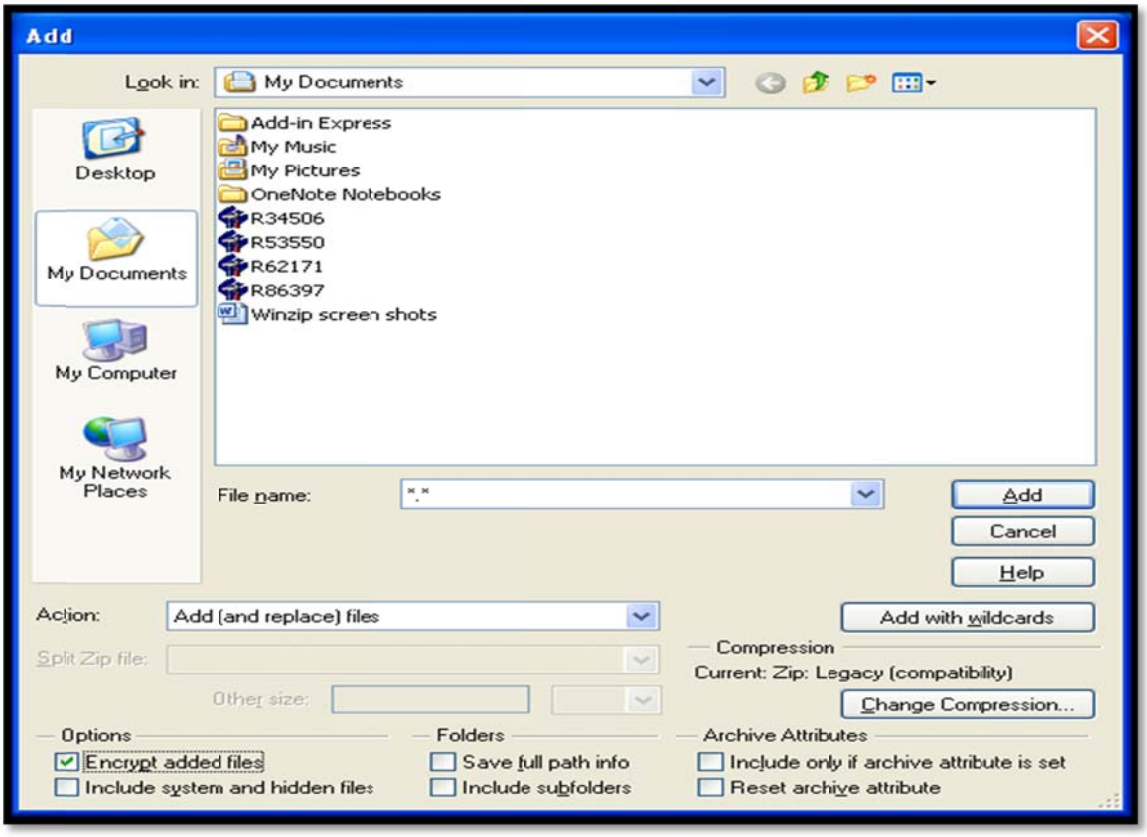
The current version of WinZip is available at www.winzip.com , it should be noted that WinZip licensing is not free of charge, to use WinZip for other than the Trial period a valid license is required. There is a version for Windows and a version for Mac.

Using the menus/toolbar

2.1. To create an encrypted zip file from the menu, select “Add” from the menu bar.



2.2. Select the documents to zip and encrypt, ensuring to check the “Encrypt added files”.

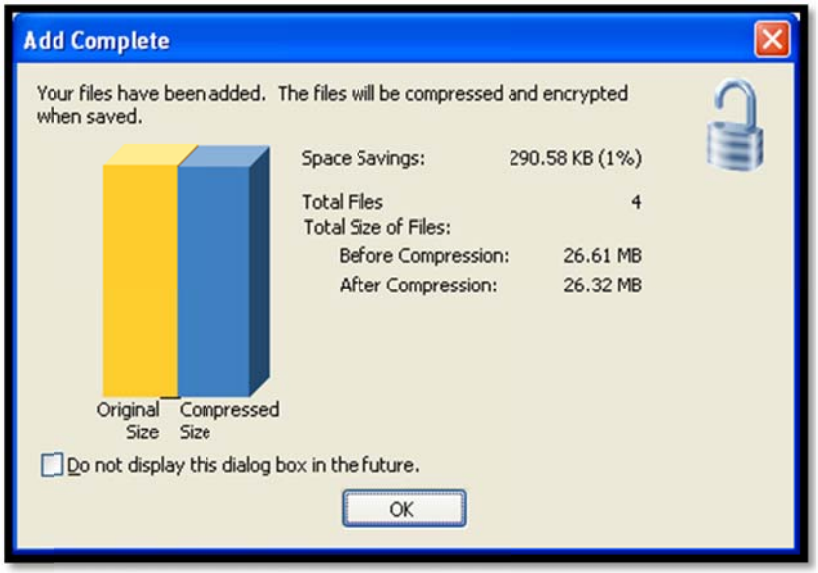


2.3. Because WinZip has three levels of encryption, the following Caution message is displayed.

2.4. If Help is selected, it will take you to WinZip's web site about Encryption and Encryption Methods.

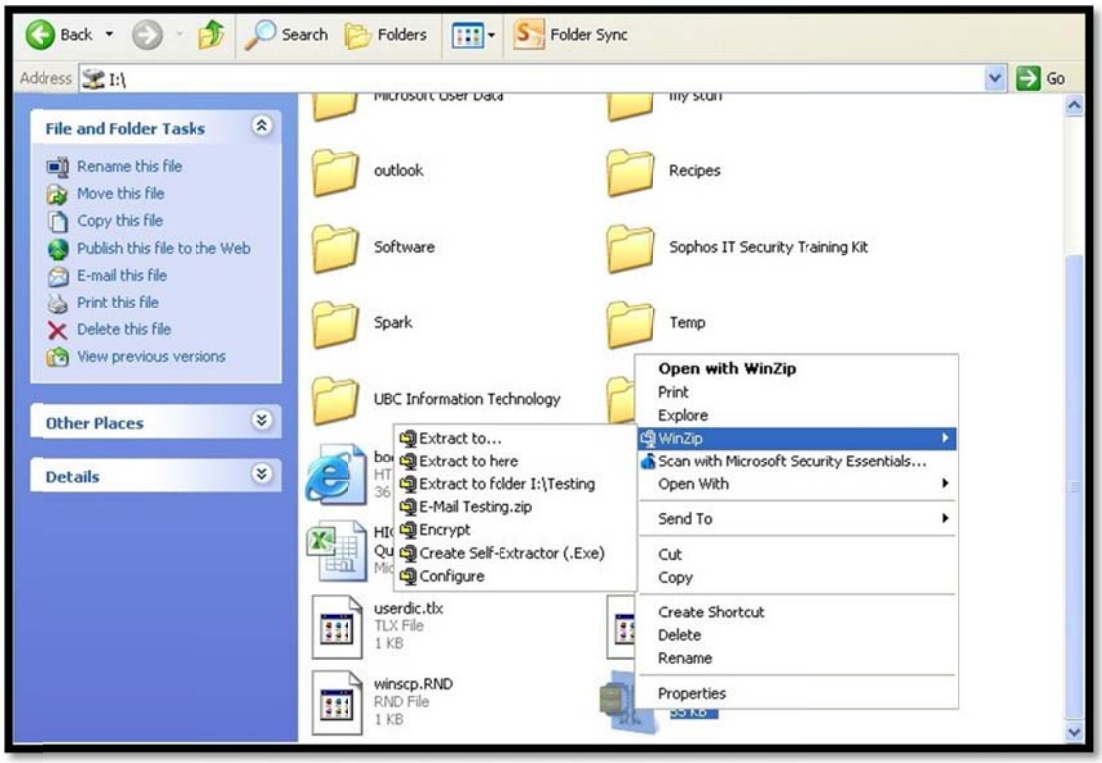
2.5. UBC's Information Security Office recommends that "256-Bit AES" be used, along with a strong password. Once the password is provided, select OK and the process will begin.

2.6. When completed this dialogue box will appear, select OK to complete the process. Your files are zipped and encrypted.



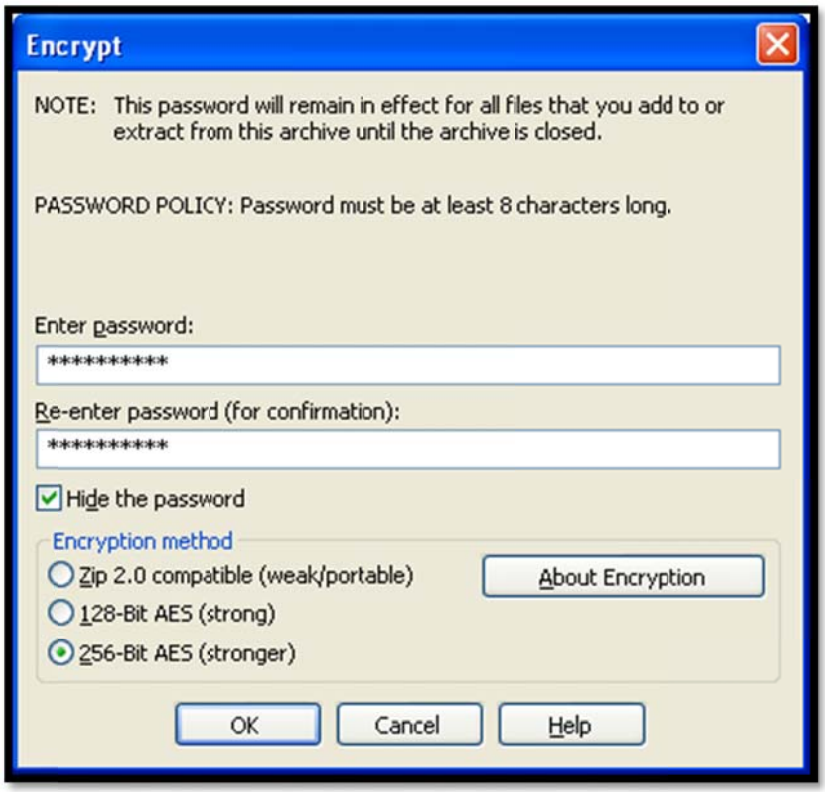
Using Window Explorer

2.7. With WinZip installed on Windows machines it is also possible to encrypt the contents of previously created zip files by right clicking on the zip file and highlighting WinZip from the pop-up menu, then selecting encrypt from the sub menu.



2.8. Again, as we have selected Encrypt the caution message appears (of course the message can be turned off).

2.9. As before, we provide a strong password and ensure that we are using 256-Bot AES, select OK.



3. How to use AES Crypt to Encrypt Files

AES Crypt is an open source application providing file level based encryption the latest version is available at http://www.aescrypt.com/

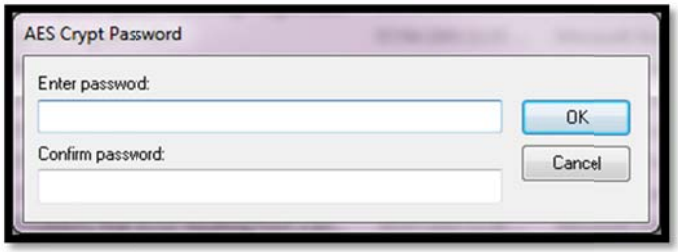
Windows

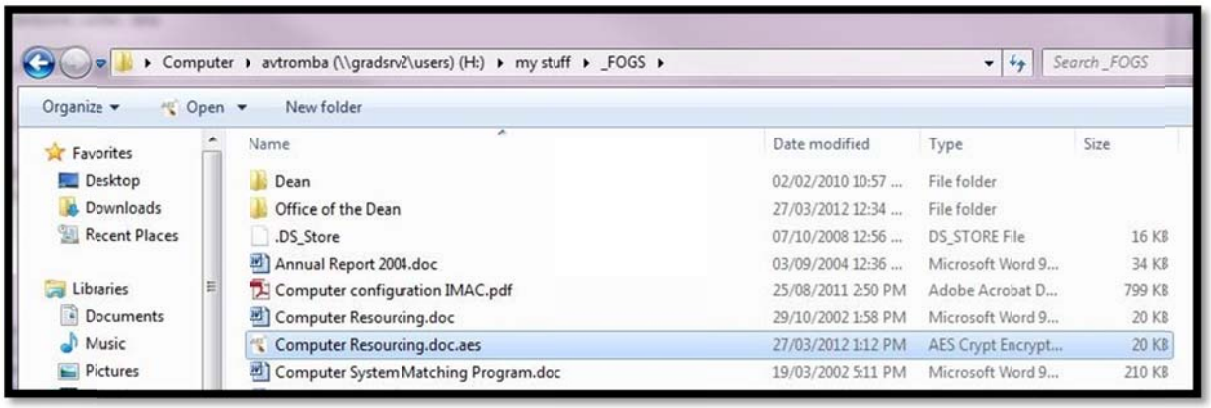
3.1. Install AES Crypt on your system.

3.2. Open Windows Explorer and select a file to be encrypted, right click on the file.

3.3. Select AES Encrypt from the menu.

3.4. Provide a strong password. Select OK, this will then create a file with the same name but with an .aes extension.





3.5. Depending upon where the original file is located it may be necessary to delete it.

AES Crypt for Mac

3.6. The Mac version of AES Crypt offers a simple to use drag and drop GUI to enable you to securely encrypt and decrypt files on your Mac. As seen below.

3.7. Make sure to provide a strong password.

3.8. An important note is that the GUI application is actually a script that executes the command-line version created for the Mac. To install the GUI application, just Click on the 'AESCrypt' package and follow the prompts.

3.9. The best way to use the tool is to drag the AESCrypt application to the Dock and drop files to be encrypted on it. To decrypt, find the file in the same directory where the original file was located, which will have an AESCrypt Icon associated with it and double click it.

Command-Line Option

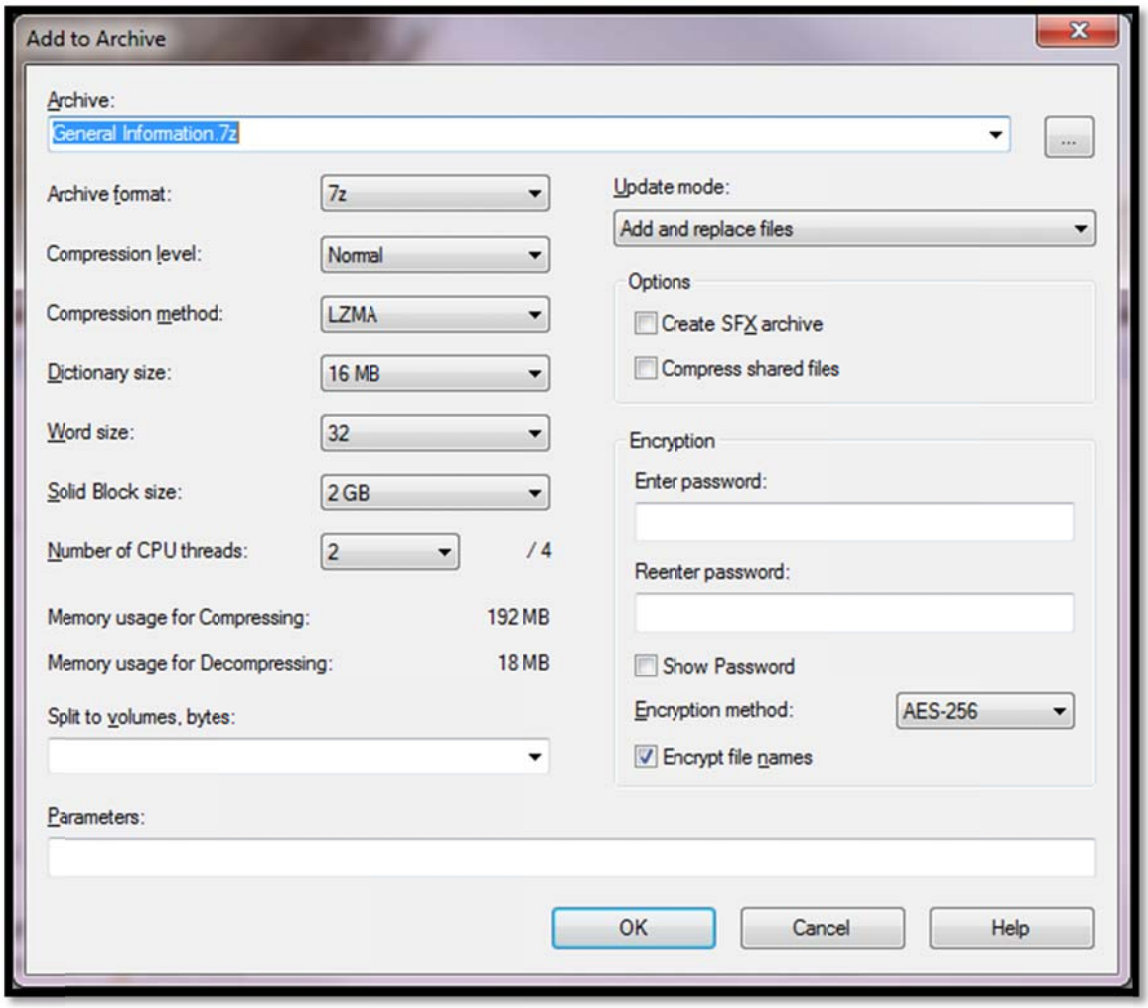
3.10. The Mac version of AES Crypt was created from the source code created for Linux. It works exactly like the Linux version. Rather than repeating much or all of the same information, please refer to the Linux page for examples of how to use AES Crypt on the Mac.

3.11. Depending upon where the original file is located it may be necessary to delete it.

4. How to use 7-Zip to Encrypt Files

4.1. Right click on the files or folder you wish to encrypt.

4.2. Select 7ZIP add to archive.



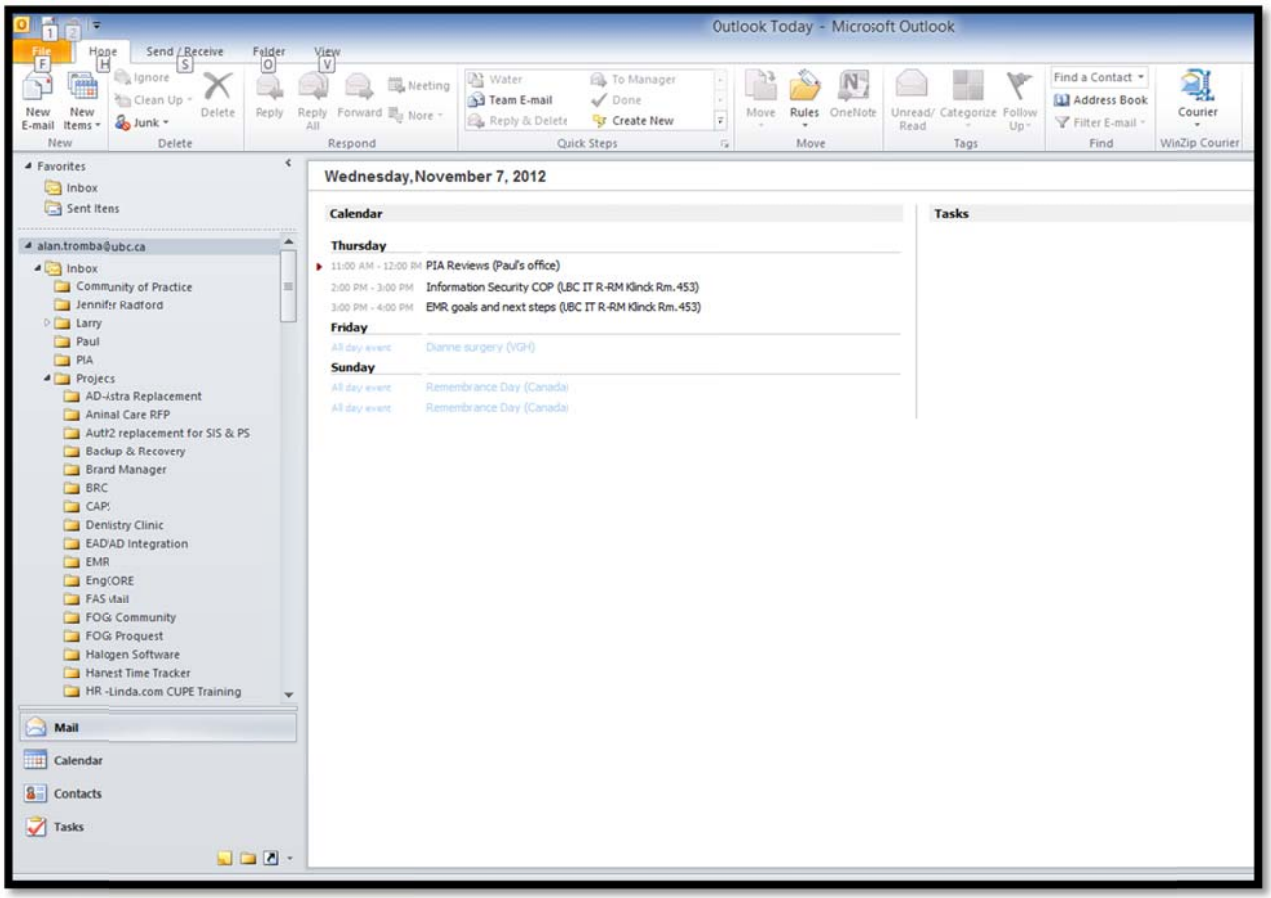
4.3. Select or create the name of the archive about to be created, leave the balance of settings as is. Note the Encryption section in the dialogue box, please provide a strong password and ensure that AES-256 is selected, and then select "OK". This creates the name of the archive with a .7z extension and will require the password to open and decrypt the archive.

5. How to use WinZip Courier to Encrypt Attachments

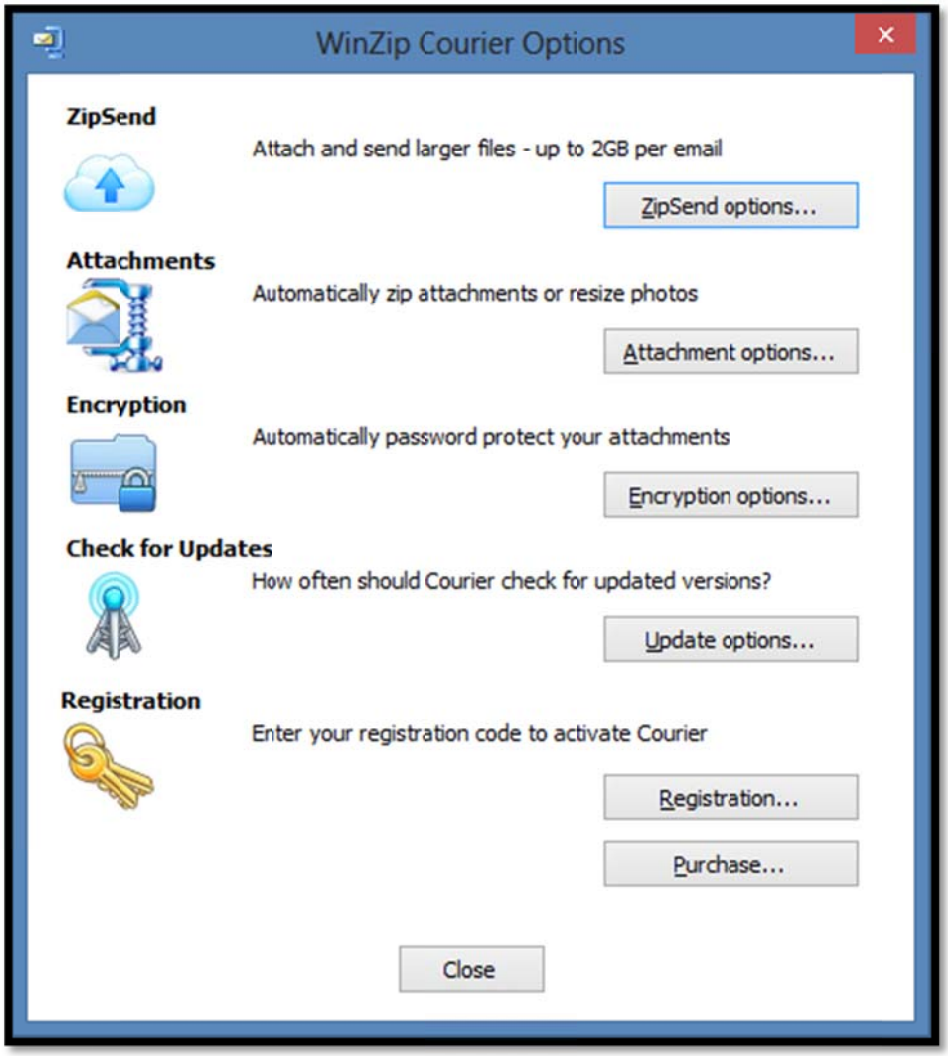
The latest version of WinZip Courier is available at http://www.winzip.com/win/en/prodpageec.htm. It should be noted this is a product that requires a paid licence.

5.1. WinZip Courier allows you to encrypt attachments as you are sending them; to do this first download and install the product.

5.2. Once installed WinZip courier will work with the following e-mails clients; Microsoft Outlook 2003, 2007 and 2010.

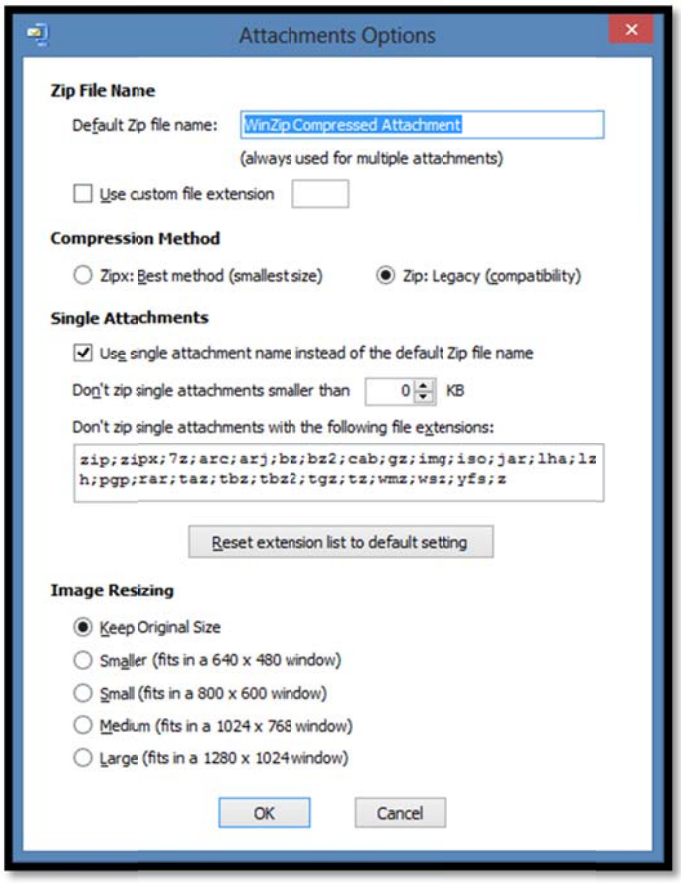


5.3. Please take note, WinZip Courier has been added to the Outlook ribbon/toolbar. Now we need to select our options for Courier.



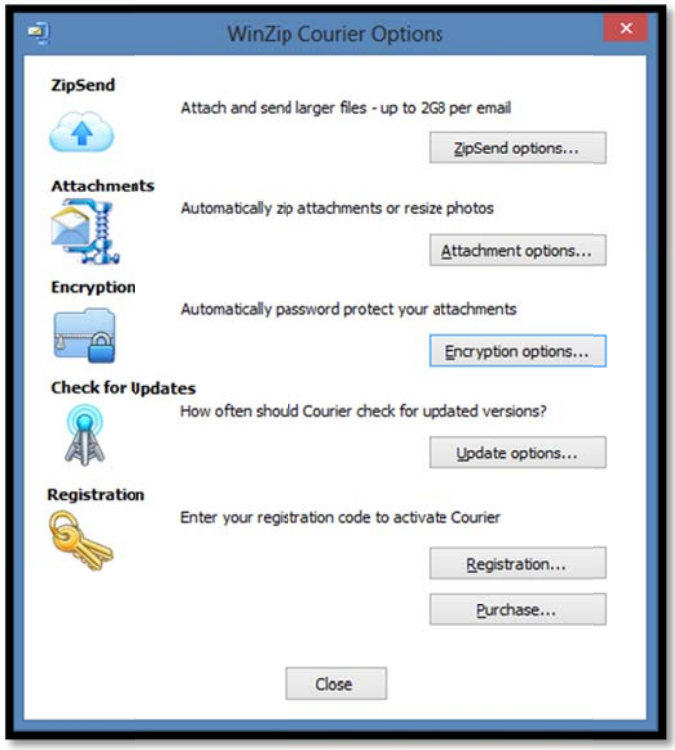
5.4. The two items on the menu we will be looking at are Attachment Options and Encryption Options. Let's begin with attachment options.

5.5. Here we have the options to set the name of the attachment to use, the Compression Method, Single Attachments and Image Resizing, we are going to accept the defaults. Next step is to look at Encryption Options.

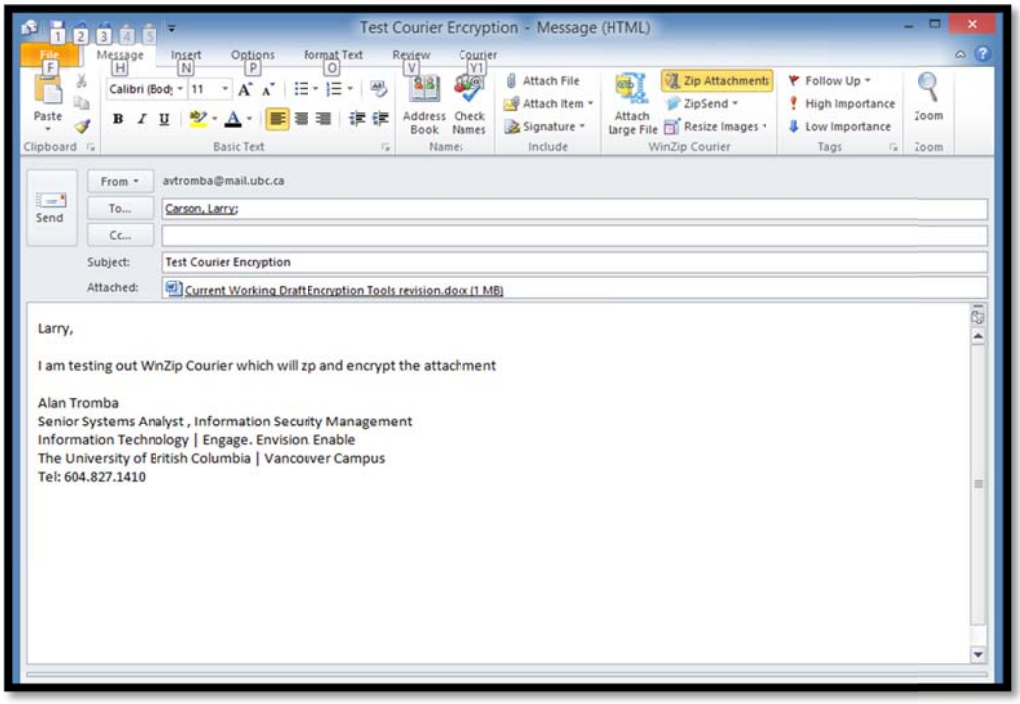


5.6. To encrypt attachments, ensure that "Encrypt Attachments when zipping" is checked and you will want to select "256-Bit AES" as the Encryption Method then click on OK. Now we have configured the Attachment Options and Encryption Options.

5.7. Click on close. We are now ready to start encrypting attachments on the fly.



5.8. Within Outlook, click on New Email and select your recipient/s, enter your subject and your message body.



5.9. The next step is to click on the Send button

5.10. Provide a strong password and ensure the Mask Password box is checked.

5.11. Select OK and your message will be sent with a compressed and encrypted attachment.

5.12. Note: Some email providers as Gmail, do not accept encrypted ZIP files attachments.

If you are a Mac user, Apimac has a product called Encrypt Email for Mac, which provides similar services as WinZip Courier, for more information here is the link to their site.

http://www.apimac.com/mac/encryptemail/

Appendix A – Encryption Product Summary

Product	Version	Windows	Mac	Linux	Availability
Microsoft Office	2007 or newer	Yes	Yes 2011	No	UBC Site License http://it.ubc.ca/service_catalogue/computers_printers/software.html
7-Zip	9.20	Windows 7 / Vista / XP / 2008 / 2003 / 2000 / NT / ME / 98	No	Command line version for Linux/Unix	http://www.7-zip.org/
AES Crypt	3.08	Yes	Yes	Yes	http://www.aescrypt.com/
WinZip	9 or newer	Yes	Yes	No	http://www.winzip.com/win/en/index.htm
WinZip Courier	4.0	32 Bit Office only	No	No	http://www.winzip.com/prodpageec.htm

Information Technology

How to Encrypt USB Sticks and Other Removable Media V1.1

Contents

Introduction

Encryption of Personal Information (PI) at UBC should be done using strong encryption, specifically AES-256 bit or equivalent; however, in order for the encryption to be strong, it must also have a strong password or passphrase. The reason for this is that if the encryption is strong then the easiest method of breaking the encryption is to "crack" the password. Short and simple passwords are easy to break while strong ones can takes years to crack.

The device most commonly used to transport PI is a USB memory stick. As with files, UBC requires AES-256 bit encryption with strong passwords or passphrases. The how-to information below will show how easy it is to encrypt a USB memory stick. It should also be noted that hardware encrypted devices are available from a variety of vendors; a list of some of the brands can be found in Appendix A.

Strong Passwords or Passphrases

A strong password in one which consists of a minimum of an 8 characters composed with upper case letters, lower case letters, numbers and symbols, e.g. "Irmb@7am."

Alternatively, you may use a passphrase with a minimum of 16 characters. This should be something easily remembered and never shared – a nonsensical passphrase is best, e.g. "Pen eats 1 pizza!" For more details, please refer to the "***Recommended Guidelines on Creating Secure Passwords***" in the UBC Information Security Manual.

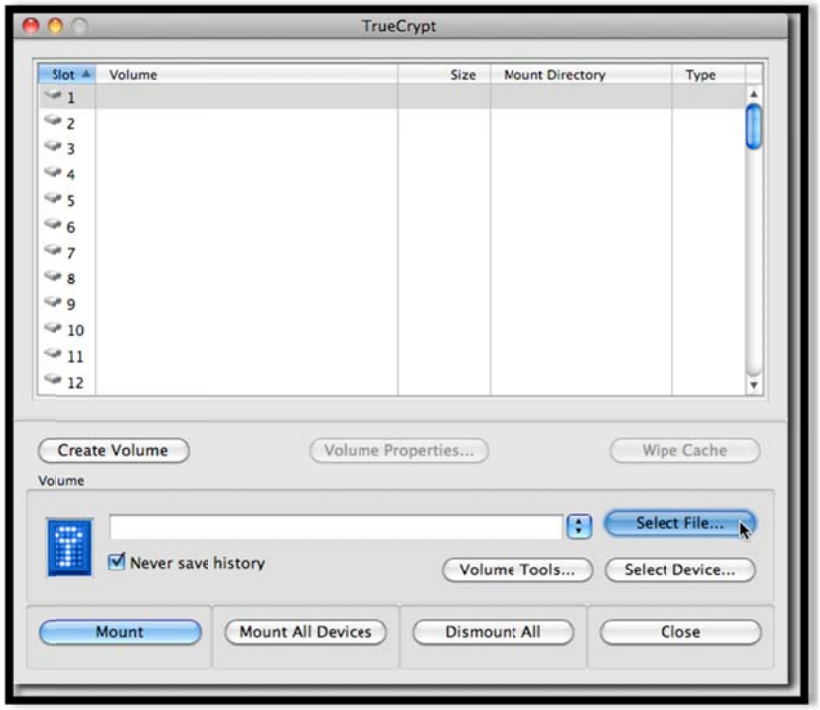
Passwords and passphrases should be changed at least every six months.

1. How to Encrypt using TrueCrypt

The latest version of TrueCrypt is available at www.truecrypt.org and is a free open-source application for performing encryption. This product has versions for Mac OSX, Windows and Linux.

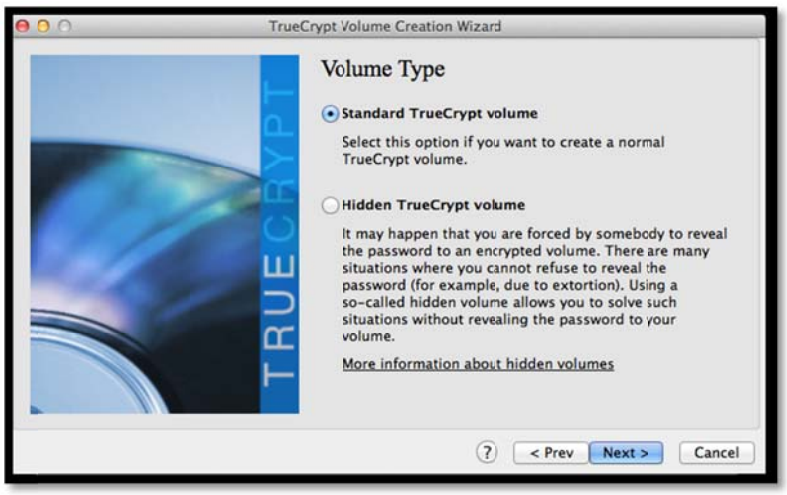
1.1. Download and install TrueCrypt using the default settings and start the program.

1.2. Select Create Volume.

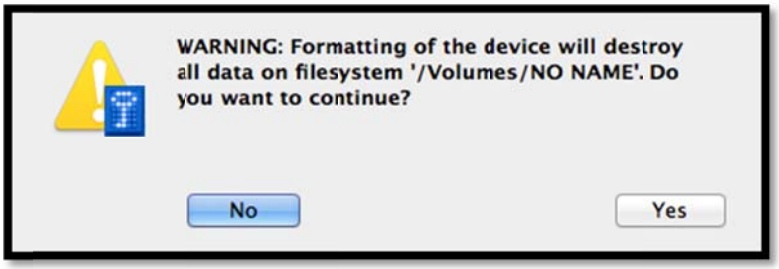


1.3. Select “Create a volume within a partition/drive” then click “Next”.

1.4. Select “Standard TrueCrypt volume” then click “Next”.

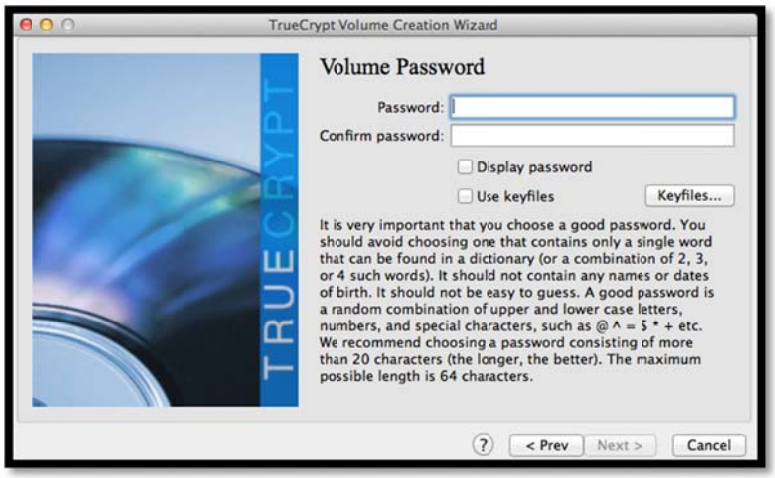


1.5. Select “Yes” to both of the following questions:



1.6. Ensure “AES” is selected as the Encryption Algorithm; any of the Hash Algorithms used in the application is acceptable. Click “Next”.

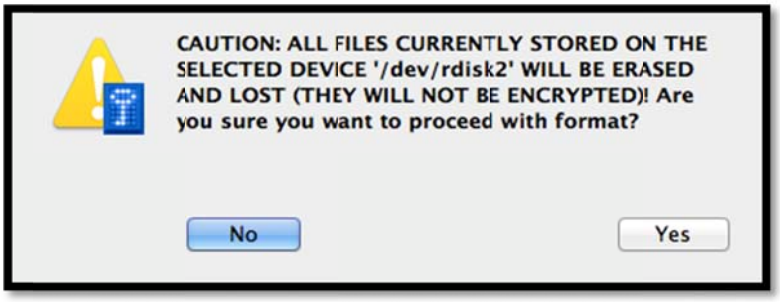
1.7. Provide a strong password, then click “Next”.



1.8. If you are planning to use the encrypted partition on systems other than Mac ones, leave the Filesystem type as FAT, click “Next”.

1.9. Click “Format”.

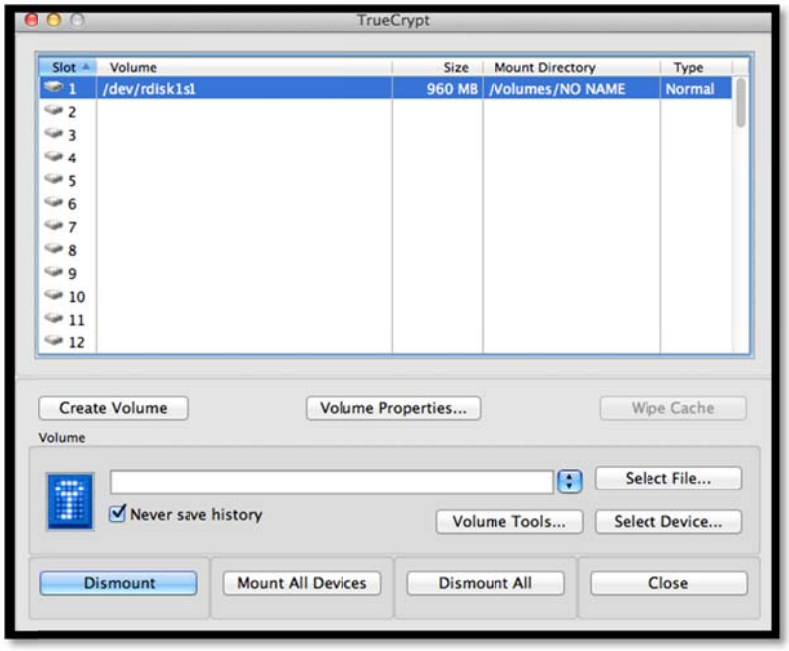
1.10. A warning appears that all data on the partition will be destroyed; select “Yes” and the formatting will begin.



1.11. Click “OK”.

1.12. Select “Exit”. Your removable media is now fully encrypted and ready to use. TrueCrypt must be installed on all systems where the media is to be used.

1.13. To use the media, have TrueCrypt running on the machine and connect the media via the USB port then select “Mount All Devices”.



1.14. You will be prompted for the password used to encrypt the device; if successful, the media will mount and you can now place your files on the encrypted media. Please keep in mind that only the minimal amount of information required should be stored on the device.

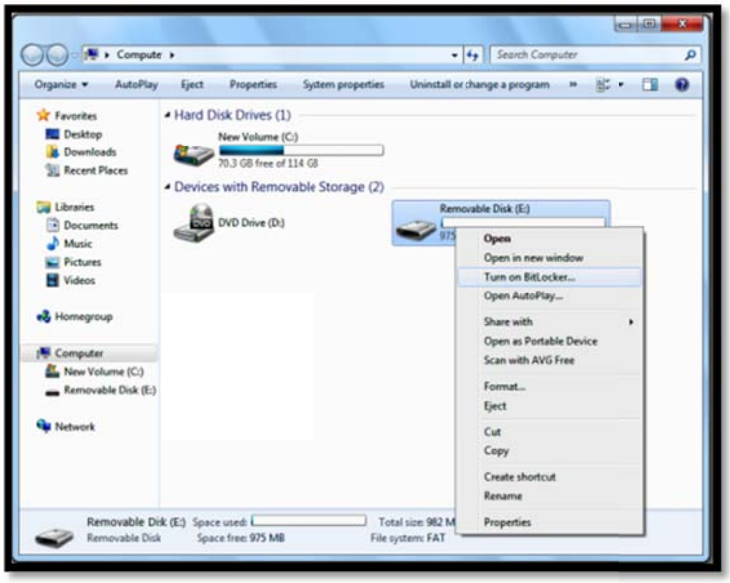
2. How Encrypt using BitLocker To Go

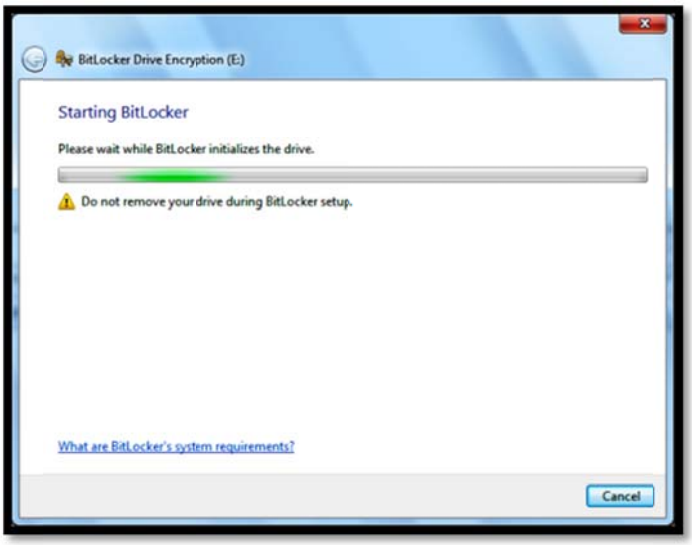
If you are using a Windows 7 or 8 based computer, BitLocker comes with your system and does not require installation. As long as you have the password, BitLocker To Go encrypted USB Memory sticks can easily be read and edited on these computers.

In addition, BitLocker To Go encrypted USB Memory sticks can be read (but not edited) on computers running Windows XP or Vista. The USB Memory stick contains a program called BitLocker To Go Reader. Once it has been installed on the Windows XP or Vista machine, you will be prompted for a password. Once the password is provided and accepted, you will be able to read the files on the USB Memory Stick. However, you will not be allowed to edit, delete or add files to the USB Memory Stick.

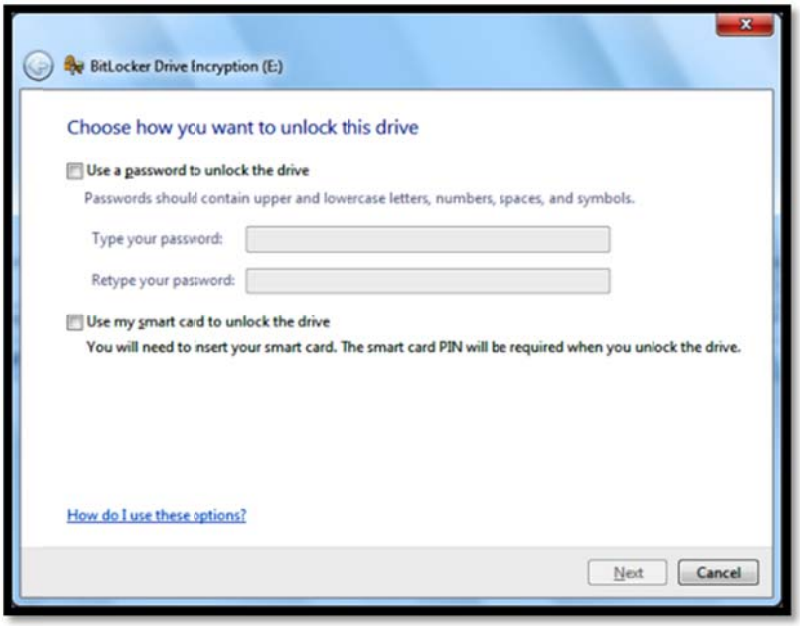
2.1. With Windows Explorer open, or My Computer, insert your USB Memory Stick in a USB port on the machine.

2.2. The USB Memory Stick should now be visible to the system. Right click on the drive and select "Turn on BitLocker" from the menu



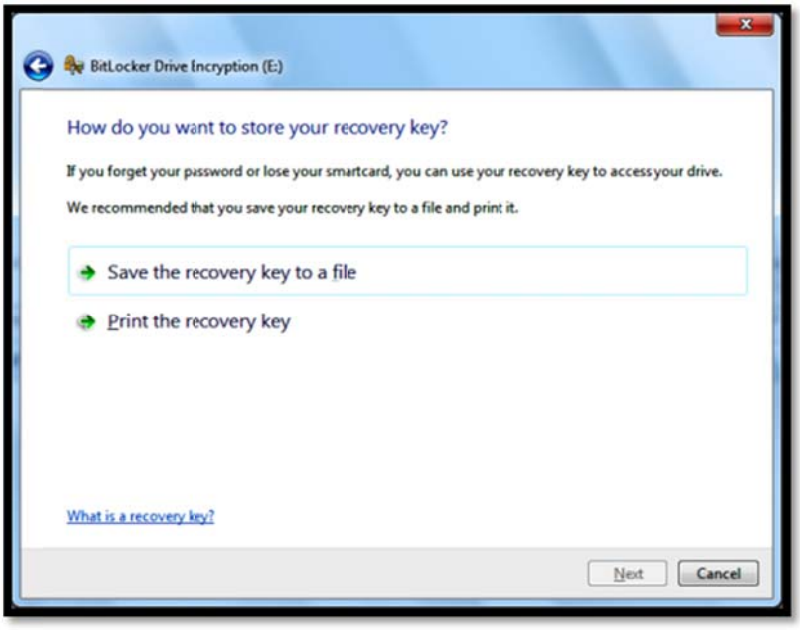
2.3. BitLocker To Go will start initializing the USB Memory Stick. This does not destroy existing data on the Memory Stick. 

When the USB Memory Stick initialization has been completed, BitLocker To Go will prompt you for a password or smart card to unlock the drive. For your purposes, you should select the "Password" option and enter a strong password or passphrase.

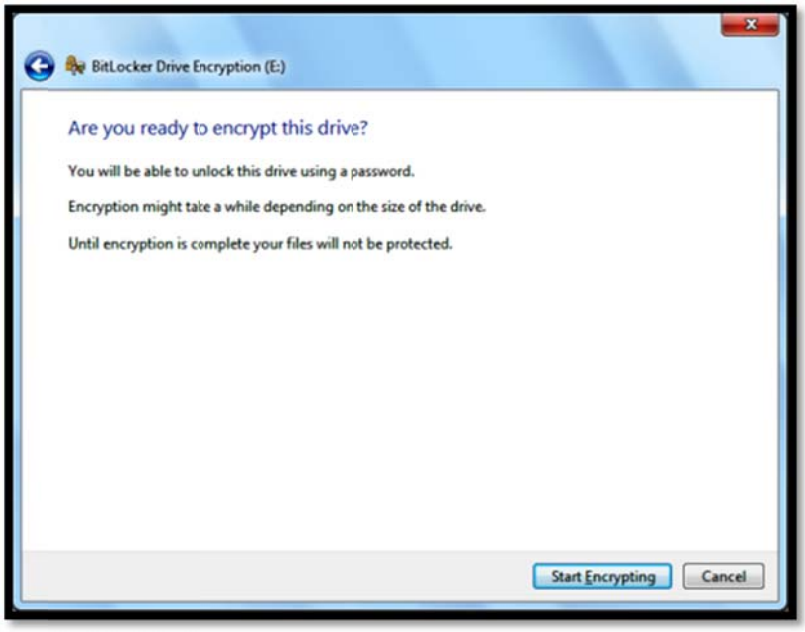


2.4. After providing a strong password or passphrase, you will be prompted for a location to store your recovery key. The recovery key will help you unlock the drive if you forget the password.

2.5. It is recommended to save the recovery key to a file on your network drive. Once the key file has been saved you will be prompted to begin the encryption process



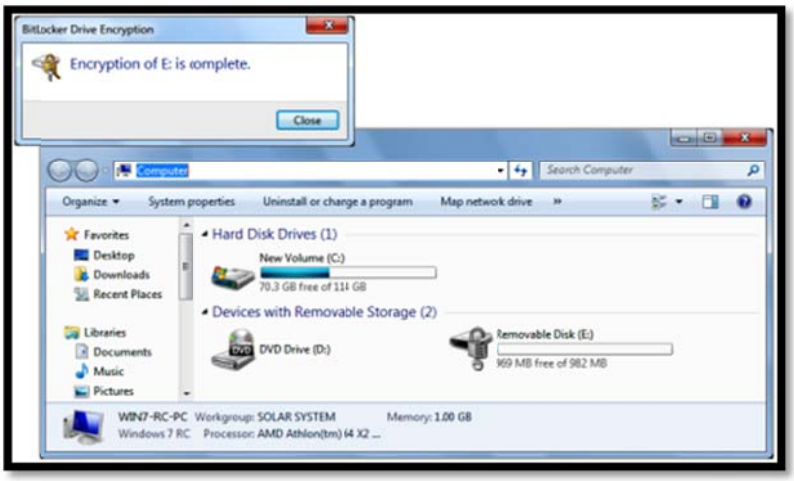
2.6. Select “Start Encrypting”.



2.7. While the USB Memory Key is being encrypted a progress monitor will display the progress of the operation. The amount of time the encryption takes will depend on how large the USB Memory Key is.

2.8. Please note there is a pause button that allows the process to temporarily stopped if you need to perform another task.

2.9. Once the encryption process has completed, BitLocker To Go presents you with the confirmation screen and changes the icon for your USB Memory stick.



2.10. The next time the USB Memory stick is inserted into a Windows PC, you will be prompted to supply the password.

2.11. Once the password has been successfully provided, select “Unlock”; the files being stored on the USB Memory Stick are available for editing or for storing additional information on the Memory Stick.

Appendix A:

Hardware Encrypted USB Memory Sticks/Drives					
Product	**Version**	**Windows**	**Mac**	**Linux**	**Availability**
Imation Powered by IronKey	Personal, Basic or Enterprise versions	Yes	Yes	Yes	http://www.imation.com/en-CA/
Kingston DataTraveler Vault	Privacy Edition, (4000, 5000 or 6000)	Yes	Yes	No	http://www.kingston.com/us/usb/encrypted_security
Kanguru Defender Series:	Basic or V2	Yes	Yes	No	https://www.kanguru.com/index.php/catalog/category/view/id/53
	Elite or 2000	Yes	Yes	Yes	