1.0 Introduction

The need to access information and perform work remotely frequently arises and presents special challenges with regard to security and privacy. In consideration of these challenges, the following requirements have been assembled to ensure a reasonable level of security and raise awareness for the need to handle sensitive information appropriately.

2.0 Scope

These requirements apply to all users and devices remotely accessing UA sensitive information.

3.0 Security Requirements

Minimum Standard Compliance
Systems and users performing work remotely must adhere to the standards outlined in the 'OIT Minimum Security Standards for Desktop Systems' document or other applicable standard published by the University.

Sensitive Data Handling
Information classified as being sensitive in nature should be handled in accordance with the security controls described in the 'UA Minimum Data Security Standards', any restrictions published by the respective MAU or data owner, and in accordance with any legal requirements pertaining to the data. For example, certain controls may require one to encrypt data while storing it, use specific encrypted/secure transmission methods, or to delete/destroy the data in a secure fashion. It is the users responsibility to be aware of any such controls and ensure their implementation.

Secure Remote Access
Remote access of sensitive information must be performed using a supported VPN technology or other secure method approved for use by the UA Chief Security Officer. For more information on remote access, please contact the OIT Support Center (see the 'Links' section).

4.0 Inquiries & Information

For more information, questions, and details regarding the above mentioned standards, please visit the OIT Security Administration website at the following link.
http://www.alaska.edu/itsecurity

5.0 Links

OIT Support Center
http://www.alaska.edu/oit/sc