IT Access and Usage Policy

For Employees, Consultants, Officer Holders & Officials

Policy Owner: Chief Finance & Operations

Policy date: January 2025

Revision number:

Date of last revision:

1. Purpose

This policy outlines the guidelines for employees regarding IT access, device usage, and data security within ISU. It aims to protect the integrity, confidentiality, and availability of ISU's IT systems and data.

2. Scope

This policy applies to all ISU employees who use ISU's IT systems, devices, and networks. The policy also applies to any consultant, Office Holder or Official granted a Microsoft 365 account by the ISU (ie anyone who had an "@isu.org or @isu.ch" email address.). Together such persons are referred to a "Users".

3. Access Management

Access Request:

Users must use ISU-approved procedures to request access to IT systems and data.

Access will be granted based on roles and responsibilities.

Access Approval:

Access requests must be approved by the Manager of the employee and the relevant Department Head or for Officers and Officials, by the Sports Department or the Director General's Office.

Only necessary access will be provided to fulfill job duties.

Access Review:

Access permissions will be reviewed periodically to ensure they are appropriate.

Changes in job roles or responsibilities must be communicated to the Department Head/HR for access review.

4. Data Security

Data Protection:

Users must follow ISU's data protection policies and procedures.

Sensitive or confidential data must not be copied, transmitted, or shared without proper authorization. All Users are formally forbidden from stocking ISU communications (emails) on personal email repositories – ie emails must not be forwarded or copied to a private email address. Should a User receive an ISU business email on the personal address they should immediately delete after forwarding to their ISU address.

Personal Vigilance and Security

Users are expected to apply personal vigilance at all times, considering whether external emails are from a reliable and known source and whether any links or attachments are safe to activate. Users should never provide their ISU login credentials to any third parties; credentials will never be requested by email by the ISU or their IT partners.

Incident Reporting:

Users must report any suspected or actual security incidents or breaches to ISU's designated IT provider or representative immediately. (currently support@evok.com) .

Unauthorized Access:

Users must not grant access to ISU devices or systems to unauthorized individuals. Devices should be secured at all times.

Unattended Devices:

ISU devices must not be left unattended in public or unsecured areas; particular care should be taken in restaurants, hotels and bars. Devices should be locked or logged off when not in use. ISU devices should never be left visible in a parked vehicle and, wherever possible should not be left in a parked vehicle at all.

Personal Use:

ISU devices and IT resources are provided for business purposes. Personal use is permitted only within reasonable limits and in accordance with ISU guidelines. High volume items (personal photos, audio or video files should not be stored on ISU devices.

Website Access:

Users of ISU devices should visit non-work-related websites with due care. Cookies should be regularly cleared. Accessing unapproved or potentially harmful sites or any website containing unsuitable content is prohibited. Accessing unsuitable websites on an ISU device or from the ISU office internet network is a dismissable offence for employees and contractors.

5. Care and Responsibility for Devices

Device Maintenance:

Users are responsible for the proper care and maintenance of ISU-issued devices. This includes keeping devices clean, avoiding physical damage, and promptly reporting any malfunctions to the ISU IT provider.

Device Usage:

Users must use ISU devices in accordance with ISU policies and best practices for security. This includes not installing unauthorized software or making unauthorized changes to device settings.

6. Remote Work and VPN Use

Guidelines

Users must use ISU-installed Virtual Private Network software to access ISU's network remotely and it is also recommended to use VPN when accessing cloud-based applications (eg Office 365). VPNs provide a secure, encrypted connection to protect data in transit.

Home Office Security

Even in your home office environment users of ISU devices should activate VPN, whether they are accessing the ISU network or not.

Employees should only use ISU laptops or other ISU devices for home office work.

Users who access the ISU cloud environment should avoid saving documents on their local drive. All officers and officials will be required to confirm deletion of all ISU documents from their devices at the end of their mandate.

.

Software and Application Use on ISU Devices

Users should only use software and applications that have been approved by the ISU. Should a User wish to install software or an application on an ISU device he or she should submit a request to IT support for approval before installing any new software. The IT team will evaluate the software for security and compatibility. Users who have mobile phones or tablets provided by the ISU may install recognized applications from the proprietary App store of their device.

7. Password Management

Password Creation

Length and Complexity: Passwords must be at least 12 characters long and include a combination of uppercase letters, lowercase letters, numbers, and special characters. Avoid using easily guessable information such as names, birthdays, or common words.

Regular Intervals: Passwords must be changed every 90 days to reduce the risk of unauthorized access. Notifications will be sent to Users when it is time to update their passwords.

Multi-Factor Authentication (MFA)

Requirement: MFA is required for accessing sensitive systems, applications, and data. This includes a combination of something you know (password), something you have (smartphone or hardware token), and something you are (biometric verification).

Setup: Users must set up MFA upon initial access and ensure that authentication methods are kept secure and up-to-date.

8. Reporting Loss or Theft:

Any lost or stolen devices must be reported to HR and Finance immediately. ISU will take necessary steps to secure data and prevent unauthorized access.

9. Termination of Access

Upon termination of employment or the end of a mandate, all access to IT systems and ISU data will be promptly revoked.

Users must return or securely delete any ISU-owned data or materials.