

THEFT OR LOSS POLICY

1. **PURPOSE:** This policy provides guidelines for reporting the loss or theft of university owned equipment. This policy will help ensure faculty and staff are aware of and protect sensitive data stored on their devices. Theft of these devices can have a negative impact on the University's reputation if the device contains sensitive data.
2. **SCOPE:** This policy applies to all technology devices purchased with university or research funds including but not limited to: laptops, tablets, phones, audio visual equipment and other peripheral devices.
3. **POLICY:** It is the sole responsibility of the university employee to take reasonable steps to protect university owned equipment from theft or loss. Employees or departments will be responsible for the replacement costs associated with purchasing a replacement device. If equipment is lost/stolen on campus the university will cover the cost of the replacement. If equipment is lost/stolen off campus it is the responsibility of the department/employee to cover the cost of the replacement. Should lost/theft of equipment occur the employee must follow these steps:
 - a. **Notify their immediate supervisor what equipment was lost/stolen:** The employee should also report a digital inventory of the data housed on the device if any. If FERPA, GLBA or HIPAA data is stored on the device, Information Services (IS) must be notified immediately.
 - b. **Notify Campus Safety:** They will investigate and take statements from the individual or supervisor reporting the incident.
 - c. **Notify the Help Desk:** An internal ticket will be generated to possibly track the lost/stolen device, take a digital inventory of what data was housed on the laptop and report any necessary FERPA or GLBA violations. If the device can't be tracked, it will be removed from inventory and a loaner device will be provided if needed.
4. **GUIDANCE:**
 - a. **Preventive Steps:** The following steps help you minimize the impact of your device getting lost or stolen.
 - Keep mobile devices physically secure at all times.
 - Do NOT store mobile devices in vehicles. Theft from cars, even when locked is the most common theft scenario for university owned mobile assets.
 - When traveling for university business, keep mobile devices on your person at all times or in a locked hotel safe.
 - Use a strong password that is not written down near your device.
 - Routinely back up your device.
 - For Apple devices enable remote wiping of your device as well as "Find My Mac"
 - Consider full disc encryption
 - b. **Data Loss:** IS needs to know what data was stored on the computer and make sure there was no sensitive, confidential or personally identifiable information on the lost or stolen device.
 - c. **Back Up Policy:** Per the University *Backup Policy*, backups of desktops, laptops, tablets and VDI's are not supported by Information Services. It is the responsibility of the faculty/staff/student to back up their systems.

5. **EXCEPTIONS:** No payment will be required of employees or their department if the equipment is stolen from their offices or other secure campus space and they have taken reasonable precautions against theft (as indicated above). If appropriate precautions have not been taken, the staff member or home department is required to pay for replacement of the computing device.

6. **SANCTIONS:** Accounts and network access may be administratively suspended by the University with or without notice when, in the University's judgment, continued use of the University's resources may interfere with the work of others, place the University or others at risk, or violate University policy. Any violation of this policy by a student may lead to disciplinary charges under the appropriate student disciplinary policy, which may include expulsion or suspension of student status. Faculty and staff violations will be addressed by their respective disciplinary policies and procedures. All known and/or suspected violations will be reported to the Vice President for University Operations. Users of University of Portland computing facilities are subject not only to University Policies, but also to applicable local, state and federal laws.