

Office of Information Security (OIS)

Authored by: Timothy Fredrick

Publish: 8/24/2021 3:25:00 PM

Last update: 5/2/2022 9:15:52 AM

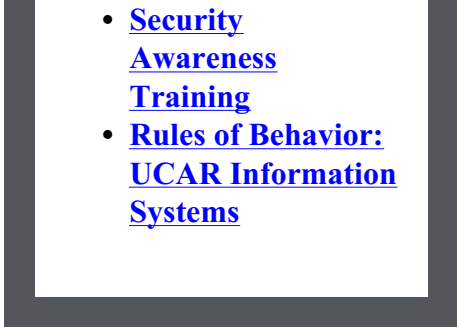
This page provides information about the Office of Information Security (OIS), OIS services, and how to request information security help.

Things to Know:

- [How to Report an Incident](#)
- [Security Standards & Best Practices](#)
- [Understanding Acronyms](#)

Quick Links:

- [Request help or report an incident](#)
- [Visit the OIS Blog](#)
- [Guidelines and UCAR Knowledge Base](#)
- [Restricted Hardware & Software](#)
- [Vendor Assessments](#)
- [Video Conferencing Guidelines](#)
- [Vulnerability Scanning](#)

- 
- [Security Awareness Training](#)
 - [Rules of Behavior: UCAR Information Systems](#)

About OIS

The [Office of Information Security \(OIS\)](#), a section of Enterprise Information Technologies (EIT), is responsible for:

- Cross-organizational cybersecurity governance and training
- Cybersecurity risk management
- Monitoring and detecting cyber threats
- Vulnerability scanning
- Incident management
- Industry security standards

We're Here to Help You

OIS strives to safeguard the UCAR Computing environment, and is available to assist you with any information security questions or concerns. For general information, please [email OIS](#).

How to Report an Incident

If you suspect a compromise involving UCAR networks, systems, or personnel please immediately contact us:

- Ext. 4300 (if calling from a UCAR extension)
- 307-996-4300 (if calling from a non-UCAR number)
- [Enterprise Service Desk](#)
- If Life Safety is involved please immediately contact: Ext.1911 to reach UCAR Physical Safety

Frequently Asked Questions

See OIS FAQs for a list of commonly asked security questions.

[How can I be secure on travel?](#)

Traveling, especially internationally, presents some additional risks to UCAR, NCAR and UCP employees and data. Mobile devices are a prime target for thieves. Hotels, airports and

rental cars or taxis/ride shares are targeted locations for professional criminals. Because of this, OIS has some recommendations to help you lower the risk of data loss or theft while traveling:

- Staff traveling to destinations that are considered high risk areas may not carry their normal work devices but must instead travel with dedicated devices issued to them for the duration of that travel.

If planning travel, please follow OIS: [OIS Travel Guidelines](#)

For more information on travel within the organization: [5-7 UCAR Travel Procedure](#)

How do I begin a vendor assessment?

To meet the organization's obligations to protect confidential information and Personally Identifiable Information (PII) / Personal Data (PD) UCAR must conduct a risk assessment for any cloud vendor or software as a service (SaaS) provider who handles or has a potential to handle employee personal records, UCAR credentials (usernames and passwords), confidential UCAR information, or non-public UCAR information. OIS teams with the Office of General Counsel (OGC) to provide a vendor security and privacy assessment (VSPA) service. VSPA documents describe risks associated with the vendor and offer recommendations for whether and how the service can be used safely.

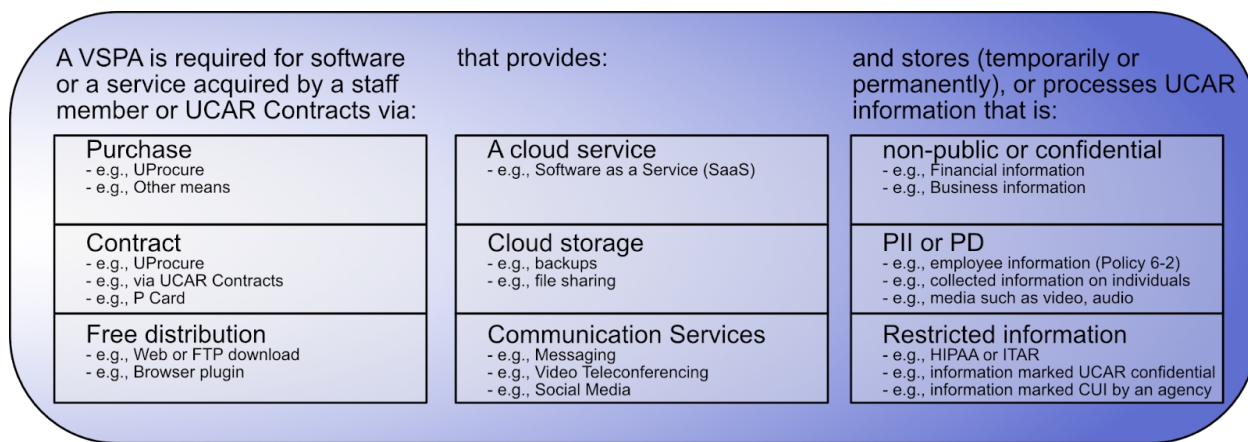


Figure 1: Determining if a Software or a Service requires a VSPA

For more information see [OIS VSPA](#) link

How do I access the VPN?

Whether you work from a traditional office, home office, your phone or tablet, or on the road, a VPN is one of the best ways to protect yourself from data breaches on the internet, especially when using public wi-fi networks. The purpose of the GlobalProtect VPN solution is to provide remote users access to UCAR network resources in an encrypted and secure manner.

For more information see [OIS VPN](#) link.

Restricted Hardware/Software

For information about what hardware is restricted in UCAR's computing environment see the [Restricted Hardware Standard](#) and the [Restricted Software Standard](#).

Assessed Vendors

For information about which vendors have been assessed and assessment results, please refer to the [Assessed Vendors List](#).

Video Conferencing Guidelines

For information about security surrounding video conferencing, please refer to [Video Conferencing](#) for specific guidelines.

Acronyms

The following assists with understanding OIS and security acronyms: [Master List of Acronyms and Terms - OIS](#)

Questions?

Contact [Office of Information Security](#).