# CrowdStrike EDR and Shared Responsibility

Using Endpoint Detection and Response (EDR) is a requirement of the campus IT standards. However, the deployment and day-to-day use of EDR does not need to be managed by OIT; users are able to self-service their EDR implementation so they can tailor it to their environment and continuously monitor for findings. When using CrowdStrike, users in a private tenant will be provisioned accounts to access the CrowdStrike management portal.

Maintaining cybersecurity best practices and compliance with all applicable laws, regulations, and policies is a shared responsibility between OIT and the user. When a user opts to self-service their EDR implementation, OIT relies on the user to carefully consider what level of protection is needed in their environment. OIT also relies on the user to take responsibility for the following tasks to manage the security posture of the environment:

- ***Install supported versions of EDR sensors to all applicable IT assets***
- ***Regularly review EDR data for endpoint detections or signs of malicious activity***
- ***Remediate vulnerabilities in accordance with the campus Vulnerability Management Standard***
- ***Provision EDR management access only to trusted individuals in your department***
- ***Report any compromised machines or active security incidents to Security@Colorado.EDU***
- ***Identify the individual who will be your point-of-contact for OIT***

Point-of-contact information:

| Name | Email | IdentiKey username |
|---|---|---|
| | | |

By signing this document, you acknowledge that you have read and agree to the above.

Signature: _____