CROWDSTRIKE ENDPOINT SECURITY SOLUTION COMPLIANCE

1. Purpose

This mandate establishes the requirements and responsibilities of Crowdstrike Falcon Prevent endpoint security solution compliance for laptop computers owned by the UNT System and its Institutions.

2. Definitions

2.1. Crowdstrike Falcon Prevent. Centrally administered and sanctioned agent-based software that detects and mitigates computer viruses, malware, and threats on computing endpoints.

2.2. Compliance. Meeting all requirements stated within this mandate.

2.3. Information Technology Support (IT Support). Individual(s) delegated as responsible for support of information technology assets owned by the UNT System and its Institutions.

2.4. Custodial Department. Department within the UNT System and its Institutions that retains possession and responsibility for the laptop computer as an institutionally owned asset.

3. Scope

This mandate applies to all laptop computers purchased by the UNT System and its Institutions.

4. Requirements

4.1 Laptop computers owned by the UNT System and its Institutions must meet the following requirements:

4.1.1. Have the current centrally administered Crowdstrike Falcon Prevent sensor installed;

4.1.2. Run currently supported operating systems and software applications; and

4.1.3. Receive regular updates and maintenance by IT Support.

5. Responsibilities

5.1. IT Manager(s) are responsible for providing the following support to laptop computers:

5.1.1. Install current centrally administered versions of Crowdstrike Falcon sensor on all laptops prior to deployment;

5.1.2. Ensure laptop computers receive updates and patches;

5.1.3. Investigate laptop computers that do not meet the standards established in 4.1. of this mandate and document variances to compliance; and

5.1.4. Resolve variances to compliance that fall within their support responsibilities.

6. Exceptions

6.1. In the event IT Support cannot resolve variances to compliance, the Custodial Department must submit a request for a security exception. The Custodial Department must submit a security exception to the UNT System Office of the Chief Information Security Officer and include the following:

6.1.1. The Custodial Department name, location, and contact;

6.1.2. The service and asset tag numbers of the laptop computer;

6.1.3. Location of the laptop computer;

6.1.4. Current use of the laptop computer;

6.1.5. Reason why the variance to compliance cannot be resolved;

6.1.6. Reason why the laptop computer cannot be decommissioned;

6.1.7. Compensating controls that mitigate the risk associated with non-compliance; and

6.1.8. Supplemental documentation that may exist in support of the request for security exception.

6.2. The UNT System Office of the Chief Information Security Officer will provide an approval or rejection of the request to the custodial department.

6.3. The UNT System Office of the Chief Information Security Officer may revoke security exceptions at any time.

7. References

7.1. UNT System Information Security Regulation 6.1000.
7.2. UNT System Information Security Handbook.

Appendix A – Document Version Log

Version	Approved By	Date	Description
1	Charlotte Russell		New Information Technology Mandate
2	Rich Anderson	2/2/2023	Updated for formatting and to reflect current endpoint security solution.