## Purpose:

To provide guidance on when malicious software controls are needed and how they should be configured.

## Standard:

1. Anti-virus and anti-malware software shall be implemented on all computing devices for which such software is commonly available. Email systems will scan incoming and outgoing messages for malicious content.
2. Updates needed for anti-virus and anti-malware software to detect new threats shall be installed within 14 days of release by the vendor.
3. Controls that only allow execution of pre-authorized code are strongly recommended, as are other configuration options to minimize the effect of malicious software such as preventing execution from temporary directories.
4. Malicious software controls should be configured to scan files and data as it is downloaded, stored and accessed, with periodic scans of all storage.
5. Malicious software controls should be configured to alert IT staff of infections, and IT staff will take prompt action to isolate or remove malicious code according to the [UF Incident Response Procedures](https://security.ufl.edu/it-workers/information-security-guide/incident-response-procedures/).
6. Malicious software controls may not be disabled or configured to reduce their effectiveness without formal authorization of the unit ISM, who will document such authorization, and require re-enabling of the controls once the authorization expires.

## References:

|  |  |
| --- | --- |
| Revision Date | Description |
|  | Policy originally adopted |
| Aug 1, 2022 | Policy updated |