Elevated Privileges Internet Restrictions

Standard ID
IOT-CS-SEC-120

Published Date
3/21/2011

Effective Date
3/21/2011

Last Updated
5/19/2017

Next Review Date
5/19/2018

Policy
06.0 Access Control (PR.AC)
06.4 PR.AC-4
06.4.1 Identity Access Management

Purpose
Limit the risk of malware infections impacting those with elevated privileges by prohibiting elevated IDs from surfing the Internet. Infections to those with elevated privileges pose much greater risk to broader and more severe negative ramifications.

Scope
IOT Supported Entities

Statement
To reduce the risk of malware or other adverse actions as a result of using an elevated account, the following controls are required:

- Internet web sites will be blocked for those with elevated privileges except for web sites "white listed" for technical support. Sites permitted will be limited to those providing direct technical support through a web interface or software fixes/patches. Sites allowed will not include technical forums or magazines.
- Submission of sites to be allowed for elevated user accounts, along with a brief justification, should be sent by a manager to the SecurityRequests@iot.IN.gov mailbox. This is a separate process from the one used to approve sites for specific individuals.

Roles
Users with Elevated Privileges

Responsibilities
Users with elevated privileges must apply best practices to minimize the risk of and from malware infections. A standard ID for basic functions (e.g., email, word processing, etc.) shall be complemented by a second ID for tasks requiring elevated privileges.

Management Commitment
Management is responsible for ensuring their personnel is in compliance with this Standard.

Coordination Among Organizational Entities
 Agencies shall coordinate with IOT where exceptions are needed.
Compliance
Bypassing or attempting to bypass these filtering exceptions shall result in discipline up to and including dismissal.

Exceptions
Exceptions may be approved by the CISO on a case-by-case basis.