COST: **$**$$ IMPACT: **MEDIUM** COMPLEXITY: **LOW**

2.D: Does the WWS immediately disable access to an account or network when access is no longer required due to retirement, change of role, termination, or other factors?

Recommendation: Terminate access immediately to accounts or networks upon a change in an individual's status making access unnecessary (i.e., retirement, change in position, etc.).

Why is this control important?

Inactive accounts may appear harmless, but they pose serious security risks when a WWS does not disable them or when accounts remain without password expiration limits. Attackers can use these accounts as the WWS may not notice their activities. Also, employees who leave the WWS could still use their login credentials to access network resources.

Implementation Tips

It can be helpful to develop a checklist for use when a person either leaves your WWS or transitions into a new role at the WWS. The checklist could include items such as returning any WWS-issued computer equipment like laptops, tablets, and smart phones, as well as deleting the individual's user accounts or changing privileges on user accounts as needed.

Resources

NIST Policy Template Guide: See Access Control Policy (1.h) Account Management. A policy document that a defined and enforced administrative process applied to all departing employees by the day of their departure that (1) revokes and securely returns all physical badges, key cards, equipment, etc. and (2) disables all user accounts and access to utility resources. *https://www.cisecurity.org/wp-content/uploads/2020/06/Identification-and-Authentication-Policy.docx*

Additional Guidance

- ✓ Terminate access to accounts and networks whenever a change in a user's status makes account and network access unnecessary.
- ✓ Revoke access for terminated and voluntarily separated employees, vendors, contractors, and consultants as soon as possible.
- ✓ Evaluate staff's need for access upon promotion or other role change within the WWS and remove any access privileges no longer required for their new role.
- ✓ Establish an off-boarding procedure with human resources, contract managers, and OT and IT staff. The procedure should include an audit process to identify accounts that the WWS should disable and delete.
- ✓ Disable an individual's physical and cyber access to WWS facilities and systems as soon as the individual no longer requires access.

WaterISAC's 15 Cybersecurity Fundamentals: Page 17 provides more information on revoking credentials. *https://www.waterisac.org/system/files/articles/15 Cybersecurity Fundamentals %28WaterISAC%29.pdf*