COST: **$**$$$ IMPACT: **HIGH** COMPLEXITY: **LOW**

**2.E:** Does the WWS separate user and privileged (e.g., System Administrator) accounts?

**Recommendation:** Restrict System Administrator privileges to separate user accounts for administrative actions only and evaluate administrative privileges on a recurring basis to ensure accurate information for the individuals who have these privileges.

## Why is this control important?

The misuse of administrative privileges is a primary method for attackers to get inside a network. If a user is logged in as an Administrator or privileged user and he opens a malicious email attachment, downloads a file from a malicious website, or surfs a website hosting attacker content, the attacker can use this access to launch an attack. The attack could include deploying ransomware or installing keystroke loggers, sniffers, and remote-control software to find passwords and other sensitive data. A second common technique used by attackers is an elevation of privileges attack by guessing a password for a System Administrator. If your utility loosely and widely distributes administrative passwords or sets them identical to passwords used on less critical systems, the attacker has a much easier time gaining full control of a system.

### Additional Guidance

- ✓ Ensure that all users with administrative account access use a dedicated or secondary account for their administrative activities. This account should only be used for those administrative activities and not Internet browsing, email, or similar day-to-day activities.
- ✓ Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access these tools.
- ✓ Set up systems to create a log entry and issue an alert when the WWS adds to or removes an account from any group that has administrative privileges. Do the same for any unsuccessful logins to an administrative account.

## Implementation Tips

Maintain an updated list/inventory of all Administrator accounts.

Review all OT and IT user accounts to determine which ones are currently set as "Standard User" or "Administrator." For those accounts that are currently set as Administrator, review whether that user requires Administrator privileges for his/her duties. If not, downgrade the user to a Standard User account. If they do require Administrator privileges, but do not currently have a Standard User account for day-to-day functions, create a separate Standard User account for that individual for day-to-day use. Restrict use of the Administrator-level account to those individuals with a need for privileged access and only used for privileged functions.

If your WWS uses Windows, there are five ways to find out what account type a user has (see Resource linked below). Knowing the account type for each user allows your WWS to determine whether there is a need to change a user's account type to allow or restrict additional privileges to perform administrative tasks.

You can also change the level of an account in a common operating system by going to "Settings > Accounts > Family & Other Users", selecting the account in question, clicking on "Change Account Type", and selecting either "Administrator" or "Standard User".

### Resources

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

**NIST Standard 800-53 Rev. 5 Access Control Policy and Procedures, AC-1:** Page 18 provides information regarding access control and access management. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

**NIST Standard 800-82r3 Guide to Operational Technology (OT) Security:** Section 6.2.1(pp. 97-108) provides additional information on role-based access control for SCADA systems. *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf*

**NIST Policy Template Guide:** See Access Control Policy (1.d) Account Management Authenticator Management. A policy document that a system-enforced policy and/or procedure requiring users to not use the same password for their General User and Administrator Accounts. *https://www.cisecurity.org/wp-content/uploads/2020/06/Identification-and-Authentication-Policy.docx*

**Windows Central:** Identifies five ways to identify the account type of users within a network on Windows. *https://www.windowscentral.com/how-determine-user-account-type-windows-10#determine_windows10_account_type_settings*