CSC

WHEN PEOPLE CHANGE ROLES—

Best Practices for Digital Assets

cscdbs.com

i INTRODUCTION

1 REVIEW

2 REPLACE

3 DEACTIVATE

4 BEST PRACTICES

INTRODUCTION

When managing company's digital assets, like domains, domain name systems (DNS), and digital certificates, one element all administrators need to keep an eye on is ***who*** has access to the portfolio and w***here*** their personal details are listed. With security incidents on the rise, and data and privacy protection laws getting stricter, it's more important than ever to keep track of user credentials and personal information in use, ensuring data is updated regularly to avoid security and compliance risks.

When people leave an organization or change roles, CSC recommends auditing all vendor portals for online assets to ensure user information is updated across all the products and services immediately.

REVIEW

We recommend a regular review of users and access levels for all vendor portals. People are the weakest link in any organization simply due to the proclivity for human error, and good user management policies are critical to retain a high level of security.

Audit your users regularly (every 90 days at minimum).
CSC Security Center℠ can help you easily view and request updates for any authorized users, and also set up notifications when new users are added.

Review your WHOIS portfolio information at least once a year.
Following the WHOIS Data Reminder Policy (WDRP), it's best to ensure your WHOIS information is current and accurate.

Review your social media accounts.

Remember to forget users.
The right to be forgotten—also known as the "right to erasure" rule—gives EU citizens the power to demand their data be deleted. It's recommended that when users leave, their personally identifiable information is removed from the public WHOIS, both due to security risks, as well as privacy and data protection regulations. CSC can help you audit all the tools and services the employee had access to and help you reduce risk by ensuring old contacts are fully removed.

REPLACE

In every organization, users are often assigned multiple responsibilities that go beyond the regular user portal access. It's important to take stock of the additional functions the person performed and make sure a proper replacement is found.

Was the employee:

- Listed as a renewal contact?
- Listed as a special notifications contact?
- Listed in the domain WHOIS contact information?
- Receiving and handling invoices for the organization?
- Associated with any security services?

Once all of these areas are identified, you can easily determine who should replace the contact and update the access information accordingly.

DEACTIVATE

As the first step, it's critical to ensure the user credentials are deactivated timely. Single sign on or federation ID set up allows you to have direct control of user credentials giving you access to quickly disable a user's credentials.

- CSCDomainManager℠
- CSC Security Center
- Brand protection portals
- DNS and digital certificate portals

It's also important to keep track of ***all*** third-party tools the employee had access to, and ensure access rights are updated accordingly.

Communicate any organization changes with your vendor partners. CSC is happy to audit the existing access rights and ensure updates are completed timely and in all available platforms. We're here to help.

BEST PRACTICES

- Keep access to vendor accounts limited to necessary users only. Ensure vendor portals allow implementation of additional security measures like two-factor authentication and IP validation.
- Consider single sign on to control user credentials.
- Consolidate vendors where possible. Fewer portals and vendor accounts also means fewer credentials to manage.
- Audit your users regularly (every 90 days at minimum). CSC Security Center℠ can help you easily view and request updates for any authorized users, and also set up notifications when new users are added.
- Ensure you have proper replacements for all contacts before deactivating them in your vendor portals.

cscdbs.com @cscdbs CSC Digital Brand Services

CSC is a service company and does not provide legal or financial advice. The materials here are presented for information purposes only. Consult with your legal or financial advisor to determine how this information applies to you.

DBS04192021