T2025_12 Immediately Remove Login Credentials and Biometric Access for Terminated Staff (April 14th, 2025)

One of the most overlooked cyber threats comes from within the organization—former employees who still have active access to systems and data. If user accounts, credentials, or biometric profiles are not removed promptly after an employee's termination, they can pose a significant insider threat. These individuals may still be able to log into systems, access sensitive files, or exploit backdoors, intentionally or unintentionally, leading to data breaches, sabotage, or compliance violations.

All login credentials including domain accounts, email, VPN, remote desktop, and cloud access should be disabled or deleted immediately upon termination. In facilities that use biometric systems (like fingerprint or facial recognition), biometric data must also be erased from all access points to prevent unauthorized physical entry. Cybercriminals often exploit gaps in offboarding procedures, knowing that organizations sometimes delay access revocation. A single forgotten or active account can serve as an entry point for ransomware, data theft, or system compromise. By implementing a well-documented, automated offboarding process integrated with HR and IT you greatly reduce the risk of internal misuse and ensure your organization maintains a strong cybersecurity posture.

References

- Geiger, E. (2025, April 3). Why is it important to immediately deactivate employee accounts and access them immediately after termination. Retrieved from Lumos. https://www.lumos.com/topic/employee-offboarding-automation-removing-access-for-terminated-employees-why-is-it-important-to-immediately-deactivate-employee-accounts-and-access-immediately-after-termination
- Hepp, S., & Hepp, S. (2025, April 11). 7 Key steps to removing access for Terminated employees. Cloud Adoption and Enablement Solutions | Retrieved from Cloudview Partners. https://cloudviewpartners.com/removing-access-for-terminated-employees/