Click Thinking Spotlight

Staffing and Cybersecurity

The decisions you make when hiring, promoting, transferring and terminating employees can directly impact your ability to maintain a cyber-secure workplace.

- Before the new hire begins, clarify access levels to digital and physical assets with IT and security so there is no confusion within the company. All new hires should also be provided with your company's acceptable use and technology policies.
- When an employee is promoted or transferred access privileges should be adjusted accordingly.
- Failure to do so can leave windows of opportunity where, for example, a transferred and potentially disgruntled employee can access areas or information that are now off limits.
- Employees can leave under a variety of circumstances. In any case, it's crucial to take timely and appropriate steps to ensure their departure doesn't compromise information security.
- The first step you should take when an employee is terminated is to notify IT and security so that access to digital and physical assets can be revoked.
- Retrieve key cards, keys, VPN tokens and other items that can be used to get past physical or digital barriers to your company..
- Arrange for a briefing with the terminated employee so you can verify that assets have been collected, including thumb drives, laptops phones or anything else of value.
- Make sure access is revoked on all system accounts, including VPN and remote access, email, networks, voicemail, online meeting apps, financial accounts and others.
- Pay special attention to revoking applications that reside outside your organization, such as Salesforce, for example.
- If the employee is leaving at an agreed-upon date, such as two weeks out, use the time to ratchet back access which can simplify the transition to termination.
- After termination periodically audit the former employee's accounts to monitor access attempts and ensure that key files or confidential resources are no longer exposed.
- Former employee accounts are frequently targeted by cybercriminals, another reason to check back.
- Any former employee who still has access to company assets is a potential data breach. The sooner access is cut off, the less likely your company will suffer negative consequences.

For the Staffing and Cybersecurity module, see your manager or information security contact.