STAFFING AND CYBERSECURITY | COVERING THE BASES

Hiring

- Clarify access level to digital and physical assets within IT and security so there is no confusion with the company.
- All new hires should be provided with your company's acceptable use and technology policies.
- They should read and acknowledge that they've received these policies and understand the rules to ensure a secure digital workplace as well as the penalties for non-compliance.

Promotions and Transfers

- Access privileges should be adjusted accordingly. It may mean new badges, key cards or digital clearances that reflect the rise in position.
- It may require the revocation of privileges in the case of a transfer.
- It may mean redefining any networks or groups impacted by the change.
- Changes should be made and communicated immediately with IT and security.

Terminations

- Inform IT and physical security.
- Notify IT so that access to digital and physical assets can be revoked.
- Retrieve key cards, VPN tokens and any other items that can be used to get past physical or digital barriers to your company.
- Conduct an exit audit to verify assets have been collected. This includes thumb drives, laptops, phones or anything else of value.
- Make sure access is revoked. This includes VPN and remote access, email, networks, voicemail, online meeting apps, financial accounts and others.
- Pay special attention to applications that reside outside of your organization, such as Salesforce, for example.
- After termination, periodically audit the former employee's accounts to monitor access attempts and ensure key files or confidential resources are no longer exposed.

Barracuda®
Your journey, secured.