5 Easy Tips for Protecting Employee Data

If you handle or maintain personal information about your employees, such as social security numbers and payroll information, you should take steps to protect that data.

If personal information about your employees is obtained by an unauthorized third party, you may be legally obligated to notify individuals and government regulators. Additionally, your expenses for investigating, remediating and defending lawsuits related to the matter can quickly add up. By taking steps to better secure your employee data, you can help protect your organization from the expenses, headaches and reputational harm that flow from a data breach. While there are many proactive steps you should consider, here are 5 practical tips you can use today to better protect your employee data:

1. **Train Your Employees on Cybersecurity Risks**.
   Well-meaning employees can be the weak link in your organization. Employees want to help, and they want to get things done, and that's what makes them a great starting point for hackers. If your employee unwittingly gives up her login credentials in response to a "phishing" email, the bad guys are on their way to accessing some sensitive employee information.
2. **Require Strong Passwords.**
   In an attempt to streamline their work, employees may be tempted to establish authentication credentials that are simple and easy to remember. That can also make them easier for the bad guys to guess! Requiring strong passwords, and requiring employees to periodically change their passwords, is a good way to further secure your systems and data.
3. **Limit Collection and Access.**
   Collect only the data you need, and allow access only by those individuals who need it for the work they do.
4. **Require Your Vendors to be Secure.**
   Your perimeter defenses won't matter if one of your vendors with access to your systems or data has lax security. Require your vendors, by contract, to maintain appropriate security.
5. **Terminate Access on Termination.**
   When someone's employment ends, you should terminate their access and require that they return all company confidential information in their possession.

If you'd like to understand more about your data security risks and obligations, and take steps to minimize the risk to your organization, please contact one of our Cybersecurity and Technology Team members.

MEET OUR CYBERSECURITY AND TECHNOLOGY TEAM

BOBBY N. TURNAGE, JR.
Team Leader
BTurnage@sandsanderson.com

DAVID G. BOYCE
DBoyce@sandsanderson.com

J. DAVID CARROLL
JCarroll@sandsanderson.com

RUTH T. GRIGGS
RGriggs@sandsanderson.com

DAVID W. HEARN
DHearn@sandsanderson.com

ERIC C. HOWLETT
EHowlett@sandsanderson.com

CHRISTOPHER K. JONES
CJones@sandsanderson.com