Letting Employees Connect Their Personal Mobile Devices Without Compromising Network Security – Ask The Expert

Implement a mobile devices acceptable use policy to protect the integrity of company and customer data

QUESTION

What policies do I need to ensure that employees who use smart phones to access company confidential data don't compromise IT network security?

ANSWER

You need a data security policy known as a mobile devices acceptable use policy outlining technical standards and rules employees must follow to connect their smart phones, laptops, tablets and other mobile devices, whether company or personally owned, to company systems and networks. At a minimum, the acceptable use policy should specify:

- The technical requirements mobile devices must meet to qualify for connection with company systems, including at a minimum, password protection and encryption capabilities;
- Access, authentication and physical security rules and protocols;
- Whatever anti-virus and anti-malware programs devices must have;
- Procedures for reporting and responding to lost, stolen or otherwise compromised devices;
- The company's authority to remotely scrub data from any such devices, even if they're personally owned by the employee;
- Employees' acknowledgment that the company will track their device access, duration and other use patterns and that they have no reasonable expectations of privacy in such data;
- Non-permissible uses or applications, such as use of mobile devices that are "rooted" or have unauthorized software installed; and
- That violations may result in discipline, up to and including termination.