Contemplating a Bring Your Own Device (BYOD) program? Consider these tips

1 Get executive buy-in for BYOD privacy protection

Getting senior management on board will ensure you can secure the resources to plan for and successfully implement a BYOD program that protects privacy.

2 Assess privacy risks

Conduct a Privacy Impact Assessment and Threat Risk Assessment before adoption to identify, prioritize and mitigate potential risks associated with the collection, use, disclosure, storage and retention of personal information, and help determine whether the benefits of a BYOD program outweigh the risks in your particular organization.

3 Establish a BYOD policy

A BYOD policy should cover acceptable use; corporate monitoring; sharing of devices with friends/family; app management; and responsibility over security features and voice/data plans.

4 Pilot your program

Before rolling out a BYOD program across your organization, test it out on select staff and on a single mobile platform first.

5 Train staff

Develop training materials and make sure end users understand your BYOD policy and that IT professionals are prepared to implement it, along with all appropriate technical security controls.

6 Demonstrate accountability

The unique challenges of BYOD demand a comprehensive and holistic approach to protecting personal information and data on all mobile devices on the network. Consider implementing Mobile Device Management software and role-based access tools as part of your privacy and security controls. Accountability also means being ready to demonstrate to employees, individuals and regulators how your BYOD program complies with applicable privacy laws and/or policies.

7 Mitigate risks through containerization

Consider partitioning devices to keep approved corporate apps and data separate from personal ones. Companies should be able to remotely and securely erase the corporate container if a device is lost or stolen, or if the employee leaves the organization.

8 Put in place storage and retention policies

For example, consider a “thin client” IT system that would allow BYOD devices to only display personal information held on corporate servers, but not store it.

9 Encrypt devices and communications

At a minimum, use up-to-date, industry standard encryption algorithms for device-to-device communications. Where devices connect to a corporate network, a secure connection is required such as a Virtual Private Network (VPN).

10 Protect against software vulnerabilities

Consider centrally managing software updates and patches to ensure systems are up-to-date and protected from malicious activities.

11 Manage apps effectively

Provide a list of approved apps that can be installed, and a policy on how apps should be installed, updated and removed. Remember, misconfigured apps can lead to data leakage or unauthorized disclosure of personal information.

12 Enable effective authentication and authorization practices

Consider a strong, centrally-managed authentication system for authenticating users and mobile devices connecting to the corporate network. This includes anybody seeking to access a device’s corporate container or to connect a device to the corporate server.

13 Address malware protection

Make sure your network security is regularly monitored, tested and updated to prevent malware attacks on mobile devices . BYOD participants should know to mitigate risk by not clicking on suspicious links, viewing suspect text messages and by exercising sound judgement as to the sites they visit.

14 Have a plan for when things go wrong

Have a formal incident management process with clear expectations and responsibilities to detect, contain, report, investigate and correct security incidents and privacy breaches in a consistent and timely manner. Maintaining an up-to-date inventory of authorized mobile devices and apps involved in the BYOD program will help manage and mitigate damage if a device is lost or stolen.

Office of the Privacy Commissioner of Canada

Office of the Information and Privacy Commissioner of Alberta

Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.