How to Create a BYOD System

Bring Your Own Device (BYOD) is an arrangement in which employers let employees use their own personal mobile devices like smartphones and tablets to conduct both personal and company business. During times of normalcy, BYOD is especially attractive for organizations that lack the budget to equip each of their employees with a computer; and in times of pandemic, it offers a relatively quick and cost-effective way to establish a network enabling large numbers of employees to work from home. But BYOD regimes can also create privacy and information security nightmares. If you follow a BYOD approach, here are 12 things you can do to manage the privacy and information security problems, based on joint guidelines from the Federal, Alberta and BC Privacy Commissioners.

1. Assess the Privacy Risks

Do a Privacy Impact Assessment (PIA) and Threat Risk Assessment to identify and figure out what to do about the risks associated with the collection, use, disclosure, storage and retention of personal information and whether they outweigh the benefits of implementing a BYOD system. Consider both the technology and procedures involved.

2. Create a BYOD Policy

Create and implement a written BYOD Policy covering (click here for a Model Policy):

- User responsibilities;
- How personal information in the organization's control may be subject to corporate monitoring on a BYOD device;
- Approved devices;
- Acceptable and unacceptable uses of BYOD devices;
- Sharing of BYOD devices with family and friends; and
- Access requests.

3. Conduct Pilot Testing

Organizations should first test their BYOD program on select staff and on a single mobile platform before actually rolling it out.

4. Provide Training

Develop and deliver materials training end user employees about the risks associated with device administration, storage and retention, encryption, app management and configuration, authentication and authorization, malware, software vulnerability and other technical issues.

5. Consider Containerization of Devices

One effective way to manage BYOD risks is to compartmentalize each device into 2 separate containers—one for employees' personal information and the other for business information. Organizations 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.

6. Implement Storage & Retention Policies

There should be written policies and procedures governing the storage and retention of personal information in the organization's custody or control. Example: A "thin client" IT system allowing BYOD devices to display (but not store) only personal information held on corporate servers, but not store it.

7. Encrypt Devices & Communications

At a minimum, organizations should use up-to-date, industry standard encryption algorithms for device-to-device communications. A secure connection like a Virtual Private Network (VPN) is a must where devices connect to a corporate network.

8. Protect against Patch & Software Vulnerabilities

Assign somebody within the organization to carry out patch management and update BYOD devices rather than count on employees to patch their own devices.

9. Manage Apps & App Configuration

Misconfigured apps can lead to data leakage or unauthorized disclosure of personal information. So, create a list of approved apps that can be installed on BYOD devices and a procedure to manage how apps are installed, updated and removed.

10. Establish Authentication & Authorization Procedures

Consider a strong, centrally managed 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.

11. Provide for Malware Protection

Take measures to ensure that BYOD devices don't transmit worms, viruses, trojan horses and other malware to company systems (and vice-versa).

12. Implement an Incident Response Procedure

Organizations should have a documented incident management process that provides for detecting, containment, reporting, investigation and correction of privacy and security breaches resulting from BYOD uses.