Acronis

BRING YOUR
OWN DEVICE

The Bring your own DEVICE (BYOD) Preparedness Checklist

BYOD Preparedness Checklist

When preparing to move forward "full steam" in to a productive mobile environment for your Enterprise, you should consider the following checklist to help in your BYOD decision-making process.

- [ ] **Create an Office of Mobility. –** Formalize a group that will coordinate the efforts needed to create, deploy and maintain a pervasive mobile strategy per the direction of the Enterprise leadership. Representatives in this group should include members from the Business, IT, Legal, HR, Sourcing/ Procurement and Operations and by under the guidance of an Executive Steering Committee.

- [ ] **Update/Document the Enterprise Information and Security Architecture.** – Define what is and what will be for content delivery and security to the new set of endpoints that will be introduced by a BYOD program.

- [ ] **Set Device Standards. –** In order to operate a successful BYOD program without sacrificing the choices of the employee, detailing and planning for a large list of acceptable device types and mobile operating systems is key. Choices of acceptable mobile technologies should only include devices that can be managed by a MDM and MAM solution.

- [ ] **Who is eligible for BYOD? –** Determine who in your company will have access to the BYOD program. Not every employee could be eligible to use such a solution based. For example, a part-time or hourly employee that access Enterprise data or email after hours in entitled to be paid for that time. This may not be acceptable for legal of employee status reasons. Appropriate use scenarios should be detailed and standards published and communicated to protect the employee and the company.

- [ ] **What content and data is accessible by BYOD? –** In most cases, not every network drive or SharePoint team site will be appropriate to allow access to all. Setting access protocols and choosing a Mobile Content Management (MCM) solution, such as Acronis Access Advanced, is key to managing the level of content collaboration needed to foster a productive workforce while ensuring secure access and sharing of vital corporate content.

- [ ] **Mobile Device Management and Security –** A major part of your effort to go mobile will be to determine how you will manage mobility. Choosing a MDM solution provider with a proven track record and strong capabilities for managing and securing devices will determine the success of your mobile strategy. An MDM solution will protect your assets from loss and unwanted access.

- [ ] **Policies and Standards –** The existing standards and polices for what is considered "appropriate use" of a device will not be the same as the ones in place for desktop and other on-premise only technologies. Mobile devices are used anytime and anywhere so the end-points for security and data loss prevention will now be pushed out to the extreme. Ensure that your standards and polices for mobility cover you fully as well as protect your employee from accidental misuse of corporate expectations due to vague or non-existent guidelines.