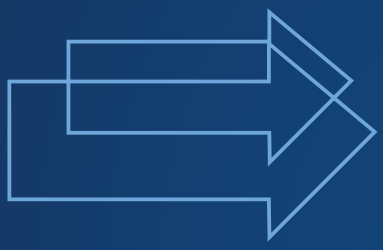
Acronis



WORKFORCE
PRODUCTIVITY

Checklist to Mobilize YOUR **WORKFORCE** and **Drive Productivity**

Enterprise Mobility Productivity 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 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.

- [ ] **Devices Standardization –** Not only will this include standards on devices (hardware and mobile operating systems) but also who will be liable for the device. This includes corporately owned as well as bring your own (employee owned). Ensure that you have included forethought in to the financial side of each of these decisions such as telco service costs, mobility management service fees, data plan costs and employee reimbursements for using personal devices for corporate activities.

- [ ] **Users –** Determine who in your company will have access to the mobility programs and what resources in the enterprise networks will be securely exposed. If mobile capabilities are not going to be allowed for everyone, a detailed mobile user/organization access strategy effort will be needed to decide who has access to what, when and where.

- [ ] **Content and Data –** In most cases, not every network drive or SharePoint team site will be appropriate to allow access to all. An information architecture strategy is required to detail which content repositories will be allowed and to whom. Mobile Content Management (MCM) and Enterprise File Syncing and Sharing (EFSS) solutions, such Acronis Access Advanced, should address all end user needs as well as the enterprise's security, management and compliance requirements.

- [ ] **Active Directory and Access Privileges –** Consider how you are currently managing your employees' access and privileges. Most mobile solutions today are only as reliable from an access perspective as determined by the access controls directed by Active Directory. Ensure that as you update polices and decisions to allow mobile access to content and data, that your AD is up to date.

- [ ] **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.

- [ ] **Mobile Device Management –** Mobile Device Management (MDM) maybe be appropriate for some organizations that want to secure and manage the device. However, as BYOD becomes more prevalent focus is shifting from securing the device to ensuring that the critical data and information assets are protected. For many organizations, secure apps and secure mobile content management (MCM) and enterprise file syncing and sharing will address the majority of needs.