baramundi

BARAMUNDI CHECKLISTS provide concise, step-by-step expert advice for handling common IT challenges in a straightforward way. You can find more checklists at: www.baramundi.com/checklists

Deploy and configure BitLocker encryption in 7 steps

Microsoft BitLocker disk encryption provides indispensable protection and security for sensitive company data. This 7-step checklist explains how to introduce and configure it precisely to meet your requirements.

Check hardware and define guidelines

Check whether end devices meet BitLocker requirements including TPM and BIOS or UEFI support, drive formats and Windows versions. Define clear usage guidelines and which devices must be encrypted, e.g., notebooks.

Step-by-step introduction and test runs

Plan a gradual rollout with testing on individual devices. Install BitLocker on all relevant devices only after you ensure that users can reliably access their devices and that there are no incompatibilities.

Central activation during OS installation

The best way to implement BitLocker is to activate it when installing the OS from a centralized admin console. This saves time on and makes the rollout easier.

Pause BitLocker when distributing software

Be sure to pause or suspend BitLocker when installing or updating certain software, 3rd-party applications and firmware, otherwise automated installations will hang waiting for a BitLocker PIN. Remember to resume BitLocker when installations complete.

Implement network unlock

Activate the network unlock function so systems connected to the company's secure network can boot automatically without a BitLocker PIN. This maintains protection while improving user satisfaction.

Save recovery keys centrally

Store BitLocker recovery keys in a central, secure location easily accessible to authorized IT team members so employees can quickly regain access in the event of forgotten passwords or hardware changes.

End user and support staff training

Inform all end users about BitLocker and its advantages. You may also need to brief them on changed login procedures. Prepare the support team to resolve problems or answer questions related to BitLocker.

In short: The successful introduction and activation of BitLocker significantly improves the security of company data. This checklist and the baramundi Defense Control module will help you complete the rollout efficiently and effectively.