

TO-DO LIST: HOW TO CONFIGURE CORPORATE PROCESSES AND SERVICES BEFORE MOVING PEOPLE TO WORK FROM HOME

1. **Configure connection to internal services via VPN**
using two-factor authentication
2. **Make sure that all the services are available outside the office and assess Internet and backup communication channel bandwidth**
3. **Install service performance monitoring system.** Software is needed for prompt notifying of specialists responsible for risk mitigation of problems in services operating.
4. **Arrange remote work:**
 - A) **on a corporate PC:**
 - Deny employee access to corporate laptop BIOS so that it couldn't boot the operating system from a flash drive
 - Enable drive encryption (Windows BitLocker or similar) on the laptops taken outside the office. And configure backup to the corporate cloud.
 - B) **on a private PC:**
 - Control operating system and software update installation, antivirus software package proper functioning; conduct malware and virus scan
 - Configure access to terminal servers
 - Provide two-factor authentication
5. **Configure the DLP system for secure working with remote employees.**
 - Install the solution on all corporate devices
 - Configure it to work in a remote mode
 - Optimise the solution's settings in accordance with the channel bandwidth
 - Activate maximum monitoring of users who can access the most sensitive information