Mitigations list :

1. EVVA MCS locks

Put an EVVA MCS lock on the director office door to prevent unwanted people from accessing this room.
Put another on the entrance door to prevent someone from accessing the office by cloning the key to the access door or lockpicking.

Cost : ~300 Euros / locks. 50 Euros / keys

2. Adding Microsoft 365 XDR

Add Microsoft 365 Security XDR to every user to reduce malware, remote access and stolen credentials risk. This also reduces OS related vulnerabilities.
Follow recommendations.

Cost : 5$ per user

3. Adding Azure MFA, credentials + application + restrict access by location

Add Azure MFA to every account, in order to connect the user will need to enter his credentials (user and password) and also validate the connection request on the Microsoft Authenticator application.
If the user is in a foreign country outside the European Union, he cannot access his services.

Cost : Azure AD Premium P2 9$ per user

4. Add Azure RDP to Server and Backup Server

Add Azure RDP to server and Backup Server, this would remove SSH related risks, and since you enabled Azure MFA, you can access the servers.

5. Enable encryption at rest on every computers

If the user is not connected or the computer is powered off, all data must be encrypted. This will lower the risk of someone stealing the data. Best way is to use Microsoft Encryption at Rest.

6. Buy a spare computer to check if USBs are infected.

Buy a spare computer with Linux, it doesn't need to be powerful at all.
The computer must be OUTSIDE of your local network, it MUST NOT be connected to the Internet in any ways.
Remove file execution permission.
Add VM on top of the computer

7. Maintenance policy update

When a computer goes to maintenance, the hard drive must be removed, this will reduce the risk of third parties accessing sensitive data.

8. Put a physical switch on the webcam

9. Computer policy

The user only has a special "personal" folder in which he can put personnel files. In this folder he can only put simple documents and he is not allowed to put restricted files defined by Microsoft 365 Security.

10. Backup server

Backup server needs to be created with VEEAM software, for the configuration you should follow the recommendation