FONDAZIONE
BRUNO KESSLER

CYBER SECURITY E SMART WORKING

We encourage all staff members in telework/smartworking to **take security precautions when using IT tools provided by FBK**.

Below are the **10 rules** we invite you to follow, together with the **guidelines for the correct processing of personal data** provided by FBK through its mandatory training on privacy protection.

1. POLICY FBK Abide primarily by FBK's **policy** and guidelines;	**2. PROTECTED CONNECTIONS** Use properly secured connections (avoid free Wi-Fi networks);
3. EXTERNAL DEVICES Use only devices (USB flash drives, external hard disks, etc.) of which you know the origin;	**4. PASSWORD** Always use secure passwords, change them periodically, keep them secret and safe;
5. TOOLS Lock your PC when you walk away from your work station;	**6. SERVICES AND PORTALS** Always disconnect from services/portals when you have finished your work session;
7. SOFTWARE Install software from official sources or repositories only;	**8. SUSPICIOUS EMAILS** Do not click on links or attachments contained in suspicious emails;
9. UP-TO-DATE OPERATING SYSTEM Constantly update your operating system;	**10. PROTECTION SOFTWARE** Make sure that the protection software (Firewall, Antivirus, etc.) is enabled and always up to date.

To learn more about cybersecurity issues, please also take a look at the **European Parliament** and the **Police Post** Tips.

The Corruption Prevention, Transparency and Privacy Unit

privacy@fbk.eu

hr.fbk.eu/en/privacy