TIP SHEET ON DATA SECURITY IN OCHA'S DATA MANAGEMENT

OCHA CENTRE FOR HUMANITARIAN DATA

INTRODUCTION

Data security is a key component of data responsibility: the safe, ethical and effective management of data for operational response. It entails a set of physical, technological and procedural measures that safeguard the confidentiality, integrity and availability of data and prevent its accidental or intentional, unlawful or otherwise unauthorized loss, destruction, alteration, acquisition, or disclosure.

This tip sheet offers a set of recommended actions for data security in OCHA's data management. All OCHA staff and supporting personnel (e.g. contractors, stand-by partners and secondments) are responsible for securing their devices and the data they manage.

PRACTICE GOOD PASSWORD MANAGEMENT

- Secure your devices and accounts with strong passwords that include numbers, capital and lowercase letters, and symbols with at least 16+ characters per password.
- Enable multi-factor authentication for all accounts.
- Do not reuse the same password for multiple accounts.
- Do not store your passwords physically (e.g. on notes) or digitally (in a file on your device) and do not share your password with others.
- Do not enable the 'Remember Me' functionality in applications and browsers.
- Change your passwords on your online accounts immediately if your device is lost or stolen.

USE ANTIVIRUS/ANTI-MALWARE SOFTWARE

- Make sure that you have appropriate antivirus/anti-malware software (Enterprise Virus Protection & Norton Product Families by Symantec Corp) on your devices.
- If you have questions about appropriate tools or how to configure them, check with the IT specialist in your office or at UN OICT.

KEEP SOFTWARE AND OPERATING SYSTEMS UP-TO-DATE

- Check regularly that your device, software, applications, and browser plug-ins are up to date and enable automatic updates for your operating system.
- Use web browsers such as Chrome or Firefox that receive automatic security updates.
- Shut down devices at the end of the day to enable updating and protect against attacks.

AVOID PHISHING SCAMS AND BE CAREFUL WHAT YOU CLICK

- When receiving suspicious emails or messages, always check the sender's address/contact information and only click on links or attachments when you trust the sender.
- Do not reply to suspicious emails or forward them to your colleagues.
- Report any suspicious activity to abuse@un.org.

USE MOBILE DEVICES RESPONSIBLY

- Where possible, use separate devices for work purposes. Keep your work devices in a secure place at all times and avoid carrying them around unnecessarily.
- Use approved messaging tools (such as Signal) that provide end-to-end encryption.
- Turn Bluetooth connectivity off when possible and minimize Bluetooth connectivity.
- Use a Virtual Private Network (VPN) when working online. The OICT Technology Standards includes two approved products: Microsoft's Always On VPN and Cisco's DMVPN. Contact OCHA Product Support (productsupportocha@un.org) for more information.
- Always sign out of your account(s) if you are using a community computer or device.
- Disable biometric unlock features—particularly when in transit.

SAFEGUARD SENSITIVE DATA AND PRACTICE DATA MINIMIZATION

- Maintain a data asset registry that indicates the level of sensitivity for each data type managed by your office. Review sensitivity levels regularly as the context evolves.
- Only collect the minimum amount of data is required to achieve the objective and purposes for a given data management activity.
- Only retain sensitive data for as long as necessary to fulfill the purpose for which it is being managed and as required by applicable guidance, law and regulations.
- Transfer and store data using approved tools and channels (locally on an OCHA server, computer or laptop; or on United Nations operated servers and systems through OneDrive, SharePoint and Teams).
- Password protect files (Word, Excel, PDF) containing sensitive data and share document passwords through separate channels (i.e. text a password for an emailed doc).
- Limit and carefully monitor the number of people with access to sensitive data.
- Define a retention and destruction schedule for all data managed by OCHA and use appropriate tools for the destruction of data.
- Encrypt your email messages (using Outlook).

KEY RESOURCES

- **UN's Information Security Awareness Training (Foundational)**
- **OCHA Data Responsibility Guidelines**
- **OICT Technology Standards**
- **IASC Operational Guidance on Data Responsibility in Humanitarian Action**
- **Guidance Note on Data Incident Management**
- **Tip Sheet on the Responsible Use of Online Conferencing Tools**

Contact Stuart Campo (campo2@un.org), the Team Lead for Data Responsibility at the OCHA Centre for Humanitarian Data, with any questions or comments.