CEPI | New vaccines for a safer world

Coalition for Epidemic Preparedness Innovations

Information Technology and Communications Policy

Objective

The purpose of this policy is to set out all employees' obligations when using or accessing the Coalition for Epidemic Preparedness (CEPI) information technology (IT) and communications systems. The policy also outlines the responsibilities of all staff in maintaining good and secure communication practice.

Policy statement

CEPI will provide each employee with the IT and communications resources needed to perform daily work. CEPI expects all resources to be used responsibly and appropriately.

General guidelines

- CEPI staff will use IT and communications facilities sensibly, professionally, lawfully and consistently with their duties, with respect for their colleagues and in accordance with this policy and the corresponding procedures.
- CEPI handles large amounts of confidential data and these should be treated (paper-based and electronic) with utmost care.
- Employees are responsible for the physical security and routine updating of antiviral software of the IT and communications equipment that has been provided for daily work. CEPI's Global Technology Officer and IT support will provide assistance as needed to assure cybersecurity standards are maintained.
- If an employee suspects there has been an IT security breach, he or she should report this to the Global Technology Officer and IT support immediately.
- Confidential documents shall not be stored on external systems, drives or devices unless prior written permission has explicitly been given by the Chief Financial Officer. This includes, but is not limited to, private tablets, phones, personal computers, thumb drives and email accounts.
- CEPI reserves the right to manage and assess that devices used to store confidential materials are at all times updated and secure and to monitor their internal processes and data traffic for security reasons.
- CEPI will not monitor an employee's use of a portable device in order to access his or her email, track his or her movements and/or access private content. However, CEPI can access an employee's work e-mail, personal space in CEPI's computer network or portable devices placed at his or her disposal for use at work, when:
    - o necessary to maintain daily operations or other justified business interest
    - o in case of justified suspicion that the employee's use of email or other applications constitutes a serious breach of the duties that follow from the employment, or may constitute grounds for termination or dismissal. CEPI will follow the all-time applicable personal data legislation regarding notice and other procedures prior to such examination.
- CEPI may remote wipe, enforce strong passwords and stop/reject apps on mobile phones and tablets, in the event of their being lost or stolen.
- Only approved storage devices with encryption may be used with CEPI laptops.

- In case of security attacks or patterns of leakage, CEPI may conduct forensics analysis on the relevant device. Failure to comply with this policy may result in disciplinary action up to and including termination.
- All IT equipment shall be returned to CEPI the last day of work, if no other agreements are made.
- The IT manager must be notified as soon as possible in the event an employee loses a portable device.
- Private use of CEPI mobile devices may be treated as taxable by some jurisdictions where CEPI employees are located. More details can be found in the CEPI Routines for mobile phones and subscriptions.

The Chief Financial Officer is responsible for oversight and maintenance of this policy, periodically reviewing associated IT procedures, and identifying any areas for improvement.

Current version	1.0
Approved by CEPI Board	January 2018
Owner	Chief Financial Officer
Flow through	N/A
Linked documents	Protection of Personal Data Policy Transparency and Confidentiality Policy
Past versions	N/A