# KEEPING YOUR HEAD IN THE CLOUDS

DEPARTMENT OF AVIATION INFORMATION SECURITY UPDATE

**Cloud Computing** is a model that allows for convenient, on-demand access from anywhere to a shared pool of computing resources and data via the internet. This includes tools and applications like data storage, servers, networking, software and databases.

In today's digital age, cloud computing has become an indispensable part of our work environment. Whether you're collaborating on projects, storing data, or using cloud-based applications, it's essential to prioritize cloud security. With cyber threats evolving rapidly, keeping your head in the clouds requires vigilance and knowledge. Here are some essential tips to ensure our cloud environment remains secure.

### 1. Use Strong, Unique Passwords

Passwords are the first line of defense. Ensure your passwords are strong—use a mix of letters, numbers, and special characters. Avoid using easily guessable information like birthdays or common words. Utilize a password manager to generate and store unique passwords for each of your accounts. NEVER share the same password across multiple accounts.

### 2. Enable Multi-Factor Authentication (MFA)

Adding an extra layer of security with MFA helps protect your accounts. MFA requires more than just a password; it could involve a text message code, a fingerprint scan, or an authentication app. This extra step makes it much harder for unauthorized users to gain access.

### 3. Regularly Update Software and Applications

Keeping your software and applications up to date is crucial. Updates often include security patches that address vulnerabilities. Enable automatic updates, when possible, to ensure you're always protected against the latest threats.

### 4. Be Cautious with Public Wi-Fi and Charging Stations

While convenient, public Wi-Fi networks are less secure. Avoid accessing sensitive information or logging into work accounts over public Wi-Fi. If necessary, use a VPN to encrypt your connection and protect your data. USB Charging stations can also be problematic and compromised. Instead, use a portable power bank that can be charged at these stations/kiosks without fear of compromising your phones data.

**5. Understand Data Encryption**
Data encryption helps protect your information by making it unreadable to unauthorized users. Ensure that sensitive data stored in the cloud is encrypted both in transit and at rest.

**6. Backup Your Data**
Data loss can occur for various reasons, from accidental deletion to cyberattacks. Regularly back up your data to ensure you can recover it in case of an incident. Verify your backups are functioning correctly and stored securely.

**7. Report Security Incidents Promptly**
If you suspect a security incident or breach, report it immediately to our IT department. Quick action can help minimize damage and protect our cloud environment from further threats.

By following these essential tips, we can safeguard our cloud-based resources and maintain a secure working environment. Your proactive approach to cloud security is crucial in protecting our data and maintaining our operational integrity.

If you have any questions concerning the above information, please feel free to contact the PHL Information Security Department. Stay secure and keep those heads (and data) in the clouds!