

Identifying Security Solutions and Best Practices

OVERVIEW

ARC has created an industry-wide cybersecurity guide to help you identify security solutions and best practices for immediate implementation.

LEARNING OBJECTIVE

Identify and implement security practices to help protect individuals and businesses from cybercrime.

Implementing Easily Accessible Solutions and Practices

Implement effective and unique electronic challenges and authentication for all login or security credentials, including but not limited to, those used to access system providers. Usernames, PIN/PCC and passwords of users accessing any agent systems that can be used to issue airline tickets may also be included in this step.

Ensure systems utilized for issuing ARC Traffic Documents and Transaction Data are purposed for business use only. Limit access to such devices through the use of biometrics or a secure password or PIN. This includes downloading software only necessary to perform activity for the business.

PASSWORD CRITERIA

- Must be 14 characters or more in length
- A combination of uppercase and lowercase letters, numbers and symbols
- A password that is different from all previous passwords and not easily guessable

MULTIFACTOR AUTHENTICATION

- Activate MFA when made available by a system provider
- DO NOT share credentials

PATCHES AND UPDATES

- Maintain installation and recording of logs of all security patches and systems updates made available by the agent's computer operation system provider and browser
- Automatic updates should be enabled

INDUSTRY-STANDARD SOFTWARE(S)

- Install and maintain antivirus software, firewall software and anti-malware software on all agents' computers
- Maintain logs for the use and upkeep of these programs

Maintenance Solutions

- Monitor the use and maintenance of effective and current anti-spam and anti-phishing email filtering systems and effective use of anti-phishing training.
- Establish appropriate maintenance of security, encryption and password protection of wireless internet systems and agents' computers.

Identifying Security Solutions and Best Practices

Guidance Solutions From the Global Distribution System

Sabre Identify

As a Second Factor Authentication (2FA), Sabre Identify helps prevent unauthorized access by validating your identity with a one-time passcode (OTP), preventing access in case your credentials are exposed to bad actors.

Sabre Identify mitigates unauthorized access; even if someone can gather your credentials, accessing Sabre or Sabre secure sites will be limited to your unique OTP.

Sabre launched a new Multi-factor Authentication (MFA) product on May 28, 2024. It is free and replaces the existing Sabre Identify product, which is being decommissioned in August 2024. Contact Sabre for more information.

AMADEUS

Secure access to Amadeus with SAAS-PASS multi-factor authentication (MFA) and secure single sign-on (SSO) and integrate it with SAML in no time and with no coding.

Log into your Amadeus services securely without ever having to remember passwords on both your computer and mobile with SAASPASS Instant Login (Proximity, Scan Barcode, On-Device Login and Remote Login).

TRAVELPORT

Please contact your account executive to see how they can support you.

Additional Resources

U.S. FEDERAL GOVERNMENT RESOURCES

- [NIST Small Business Cybersecurity Corner](#)
- [FTC Cybersecurity for Small Business](#)
- [National Cyber Security Alliance \(NCSA\) Small & Medium Sized Business Resources](#)

The Federal Communications Commission (FCC) Office of Communications Business Opportunities provides internet links to information about government agencies and private organizations with educational resources and cybersecurity tools. These descriptions and links are for informational purposes only. The FCC does not endorse non-FCC products or services and is not responsible for the content of non-FCC websites, including their accuracy, completeness or timeliness.

- [Global Cyber Alliance's \(GCA\) cybersecurity toolkit for small businesses with free cybersecurity resources](#)
- [What Small Business Owners Need to Know About Cybersecurity, Entrepreneur Magazine](#)
- [3 Biggest Cybersecurity Threats Facing Small Businesses Right Now, Entrepreneur Magazine](#)
- [Microsoft Cybersecurity Tips and Technology for Small Businesses](#)
- [FICO and U.S. Chamber of Commerce Assessment of Cyber Security Risk Report](#)

The following resources are available to help protect businesses and promote cybersecurity:

- [Payment Card Industry Security Standards Council](#)
- [Center for Internet Security](#)
- [National Institute of Standards and Technology](#)