WORKING FROM HOME OR REMOTE DURING THE COVID-19 CRISIS

Cybersecurity Best Practice Guidelines March 2020

Cybersecurity is the shared responsibility of every (government) department, employee, advisor, and collaborator. YOU play a key role in properly safeguarding and using private, sensitive information and government resources. The Government of Aruba counts on your commitment in making sure government and citizen data is properly safeguarded, and is not damaged, lost or stolen. The following Cybersecurity best practice guidelines - *Do's and Don'ts* - help remind us all of actions we must take to remain vigilant. Please note this list is not meant to be exhaustive and may be updated from time to time. Cybersecurity is all about safeguarding the Confidentiality, Integrity and Availability of our information.

Be Safe!

General

Do's

- **DO** familiarize yourself with the *Veiligheidsdienst Aruba* Basic Cybersecurity Hygiene guidelines.
- **DO** immediately read all emails sent by *Departamento Recurso Humano* related to Cybersecurity.
- **Own** your online presence, limit how much information you share on social media. Check your privacy and security settings regularly.
- **DO** report all suspicious activity and cyber incidents to your manager and/or designated IT/security representative.
- **DO** escalate cyber incidents immediately to *Veiligheidsdienst Aruba*. This is the responsibility of the Director (or equivalent function) of the department.
- **DO** automatically lock your computer and mobile phone when not in use. This protects data from unauthorized access and use.
- **DO** challenge strangers whom you may encounter in the office. Keep all areas containing sensitive information physically secured, and allow access by authorized individuals only.
- **DO** practice extreme caution when visiting COVID-19 (Corona virus) websites by non-official sources or when downloading apps on your mobile devices and refrain from checking out websites from untrusted sources. There are many ransomware apps currently circulating. There are also many fake COVID-19 websites on the web.
- **DO** be aware of WhatsApp scams and do not click on anything you do not trust or have not verified.
- **DO** practice caution when using digital calling or conferencing apps like Zoom or Skype and check your privacy and security settings.
- **Do** encourage you team to learn more about Cybersecurity.

Dont's

- **DON'T** leave devices unattended. Keep all mobile devices, such as laptops and cell phones physically secured. If a device is lost or stolen, report it immediately to your manager and/or designated IT/security representative.
- **DON'T** post any private or sensitive information, such as credit card numbers, passwords or other private information, on public sites, including social media sites.
- **DON'T** be tricked into giving away confidential work/government information. It's easy for an unauthorized person to call and pretend to be an employee or business partner.
- **DON'T** respond to phone calls or emails requesting confidential data. Always report these to your manager and/or designated IT/security representative.
- **DON'T** use 'corona virus maps' to keep track of Covid-19.
- **DON'T** send unverified information to your friends to "warn" them. This is how malware and fake news propagates.

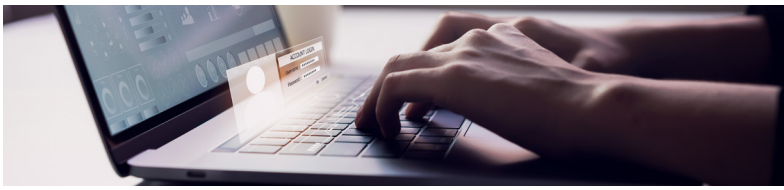
Email, Passwords and Social Media

Do's

- **DO** use hard-to-guess passwords or passphrases. A password should have a minimum of 12 characters using uppercase letters, lowercase letters, numbers and special characters. To make it easy for you to remember and hard for an attacker to guess, create an acronym. For example, pick a phrase that is meaningful to you, such as "My son's birthday is 12 December, 2004." Using that phrase as your guide, you might use Msbi12/Dec,4 for your password. We also recommend creating password phrases in Papiamento.
- **DO** use different/unique passwords for different accounts. If one password gets hacked, your other accounts may not get compromised.
- **DO** keep your passwords or passphrases confidential. You can use secure password vaults approved by your manager and/or designated IT/security representative.
- **DO** use privacy settings on social media sites to restrict access to your personal information.
- **DO** enable two-factor authentication password when possible.
- **DO** pay attention to phishing traps in email and watch for telltale signs of a scam.
- **DO** use encryption for email attachments with a password (e.g., 7zip AES) if you have to send sensitive information.

Dont's

- **DON'T** put sticky notes with your passwords on them below your keyboard or behind your screen/monitor.
- **DON'T** share your passwords with others or write them down. You are responsible for all activities associated with your credentials.
- **DON'T** share user credentials via unsecured, unencrypted media such as email. Use password managers if needed.
- **DON'T** open mail or attachments, or click links from an untrusted source. If you receive a suspicious email, the best thing to do is to delete the message, and report it to your manager and/or designated IT/security representative.
- **DON'T** open attachments send via email without first scanning it for virus, malware, spyware, Trojans etc., even if you know the sender. This can be automated.
- **DON'T** click on links from an unknown or untrusted source. Cyber attackers often use them to trick you into visiting malicious sites and downloading malware that can be used to steal data and damage networks. Many attacks are happening daily around the world and attackers are using Coronavirus or COVID-19 topics as 'bait'.
- **DON'T** send any private or sensitive information through email unless authorized to do so.



Paper and Printing

Do's

- **DO** abide by a clean desk practice.
- **DO** destroy information properly when it is no longer needed. If it's on paper, use a crosscut shredder if available. For all electronic storage media, consult with your manager and/or designated IT/security representative.
- **DO** be aware of your surroundings when printing, copying, faxing or discussing sensitive information. Pick up information from printers, copiers or faxes in a timely manner.
- **DO** practice private printing where possible to make sure that your documents will not remain on the printers.

Dont's

- **DON'T** leave sensitive information lying around the office or house (or your current place of work).
- **DON'T** print if you can avoid it.
- **DON'T** leave printouts or portable media containing private information on your desk or table. Lock them in a drawer to reduce the risk of unauthorized disclosure.

Public WIFI and Bluetooth

Do's

- **DO** remember that wireless is inherently insecure.
- **DO** consider using a paid Virtual Private Network (VPN) for enhanced secured connections if possible.

Dont's

- **DON'T** connect to any and all public/open WI-FI without proper VPN. Only use VPNs that have been approved by your manager and/or designated IT/security representative.
- **DON'T** leave wireless or Bluetooth turned on when not in use on any device. Only do so when planning to use and only in a safe environment.
- **DON'T** use Bluetooth in public spaces.

Work (Desktop) Computer, Laptop, Tablet, Mobile Phone

Do's

- **DO** lock your screen when leaving your device, even at home.
- **DO** make sure you update (automatically) your operating system of all your digital devices.
- **DO** keep a clean machine. Make sure you keep all your software and internet-connected devices upto-date to reduce the risk of malware infection.
- **DO** use up to date anti-virus to check external drives (e.g. USB) before opening files on work computers, laptops and tablets.

Dont's

- **DON'T** install any freeware/applications that are not directly needed for your daily work.
- **DON'T** install unauthorized programs or apps on your work desktop computer, laptop, tablet or mobile device. Malicious applications often pose as legitimate software. Contact your manager and/or designated IT/security representative to verify if an application may be installed.
- **DON'T** install mobile applications from untrusted sources. Contact your manager and/or designated IT/security representative to verify if an application may be installed.
- **DON'T** plug in portable devices (e.g., USB) without permission from your manager and/or designated IT/security representative. These devices may be compromised with code just waiting to launch as soon as you plug them into a computer.
- **DON'T** insert unknown or found USB devices into your computer and report this to your manager and/or designated IT/security representative.