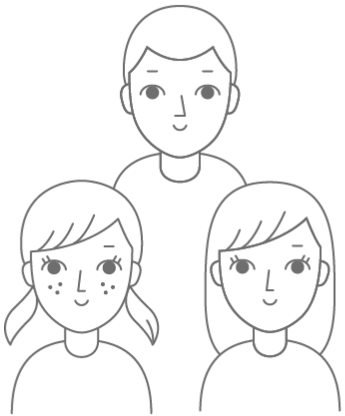
OP Financial Group's Security Guidelines for Partners and Contractors remote working within Corona situation

Information in various forms

- Information is found in various formats, such as thoughts and speech. Information can also be printed out on paper or recorded electronically. Information needs protection in all of its forms.
- Information security is often considered something that is solved by information technology. However, in practice, you are our best defender and you can affect information security significantly with your behavior and by acting safely. This means following agreed instructions and processes, and you will help a lot by reporting any deficiencies you come across.

Thank you for being our information security defender!



Confidentiality and its agreement

- All of OP Financial Group's (later OP) employees and the partners, subcontractors and consultants working on OP's behalf must have a confidentiality agreement made in conjunction with their employment contract or other agreement. The agreement must to be on the same level as OP's own.
- You as an OP's subcontractors employee have undertaken to keep secret all matters applying to the financial position or state of health of OP and its customers. This confidentiality obligation is in force throughout the employment relationship and thereafter, based on a contract as well as various regulations. Confidential information includes business and trade secrets.
- Confidential matters must not even be disclosed to other employees within your organization except in the extent required by work duties.
- Handle, collect and process OP's information that is necessary to perform the service ordered by OP and only on the extent required by these services.

Confidentiality when working

- You need to understand what the confidentiality level of the task you are doing is at any given moment.
- Tasks need to be designed and executed so as not to compromise the information security and privacy of information and customer secrecy.
  - If any of these starts to be compromised, the handling of the work related information needs to stop. Move and continue working on a safer place. If this is not possible, handling of work related information need to be terminated until surroundings are safe to continue.
  - Work related to OP must not be done when there are unauthorized persons present to hear or see information related to OP.
- Always check the identity of the person who will be receiving information. This must be done in customer service situations, on the phone and in email conversations.

Information security classification

- The aim of information security classification is to guarantee the confidentiality of the information required for OP's operations.
- Information security classification is an important part of the life cycle management of information and information material.
- Information must be handled at the level required by the security classification defined for it.
- Information shall only be handled by the personnel authorized to handle it and the personnel of partners and subcontractors working under related assignments.
- Information must not be provided to other personnel of partners or subcontractors for further handling without authorization and same level security agreements and awareness training.

Security when working

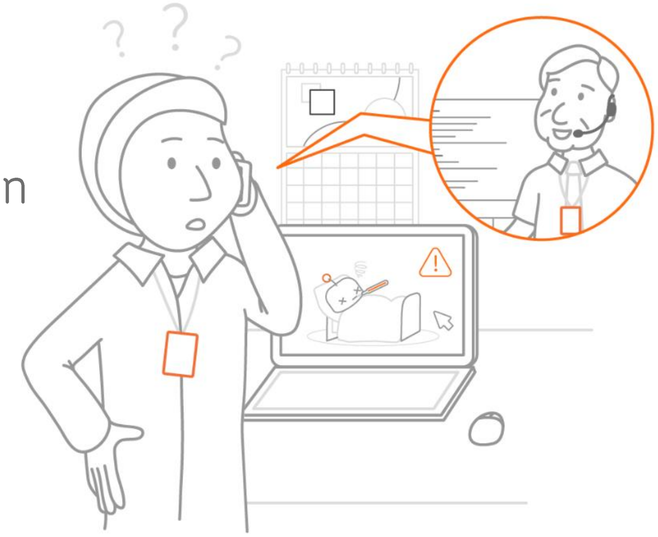
User names and passwords

- Access rights are used to ensure that information stored in documents and information systems related to work and customers can only be used by the persons who need it for their work.
- In order to use information systems and workstations you must have a personal username and password. Access rights granted to employees enable access only to information they need to perform their work.
- Use only passwords that cannot be easily guessed for your work. Make sure each of your accounts has a separate, unique password. Consider using a password manager to securely store all of them for you. Passwords need to be built from at least 15 letters.
- When work duties change, access rights must be reviewed and, if necessary, changed. At the end of a work relationship, access rights must be removed. If you know that your user rights are more extensive than your duties require, tell your supervisor.
- You have your own role based access rights and you are responsible of actions done with them.

When working remotely

- The same guidelines need to be applied when working in the office or outside of it.
- Work only with your employer’s computer or mobile devices and services.
- When working, do not tell you are working remotely or your location.
- As far as possible, do not mix work and leisure activities on the same device.
- Work related to OP must not be done in public areas or when there are unauthorized persons present to hear or see information related to OP. All of those are unauthorized persons who do not work with OP as a customer.
- Under no circumstances should the confidentiality of information be compromised and working spaces should always allow secrecy to be maintained.
- Don’t let someone else to use your access rights by leaving your computer unlocked.

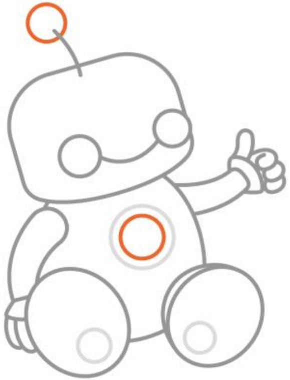
When working remotely



- Familiarize yourself of your organizations processes on areas such as
  - reporting stolen device. You need to know what to do and where to call in such situation.
  - reporting security incidents. You need to know what to do for a possible security incident. Where do you report them and get help with response activities?
- One of the most effective ways you can protect your computer at home is to make sure both the operating system and your applications are patched and updated. Enable automatic updating whenever possible.
- At home you may have different kind of appliances and gadgets available. Do not connect those or any unknown (USB) devices to your work devices. They may spread malware or steal information.

When working remotely

- Use your own networks and secure VPN connections. Do not use connections such as public and open WLAN networks.
- The most effective steps you can take to secure your own wireless network is to change the default admin password, enable WPA2 encryption and use a strong password for your wireless network.
- Be aware of all the devices connected to your home network such as gaming consoles, TVs and appliances. Ensure all those devices are protected by a strong password and/or are running the latest version of their operating systems and not jeopardize your work devices and information.



When working remotely

- Your workspace needs to be sufficiently soundproof so that outsiders who are not relevant for work for OP (e.g., your own family members) cannot hear any confidential discussions (discussions with OP or colleagues).
- Limit the workspace from other people as much as possible and confidential work related to OP and its services for times there are no other people present (e.g., a separate workroom).
- Your workspace should be located in a place where outsiders who are not relevant for work for OP cannot see any confidential information (also consider visibility from windows).
- In principle, all customer information that is handled when working remotely must be saved in a digital format. Regardless, if some customer information happens to be physical for one reason or another (e.g., notes written on paper), it must be stored in a secure and locked location that cannot be accessed by outsiders.

Sanctions procedure regarding possible information security violations

- In the OP, information security violations refer to actions that do not comply with documents provided in relation to management and control models and concerning information security, cyber security and data protection, actions against any guidelines provided by the Group companies or institutions.
- The sanctions applied to consultants, temporary agency workers and other cooperation partners may include the following: temporary restrictions of access rights to information systems (closing user accounts), agreement termination by giving notice or cancelling in accordance with the agreement terms, any other sanctions in accordance with the agreement terms (such as indemnification liability) and reporting an offence (acts punishable by law).
- The manager of the responsible function decides whether the user accounts of a consultant, temporary agency worker or other cooperation partner are closed, their agreement terminated, or other sanction options used.

About OP:s technical security infrastructure and information security incident response

- In banking and insurance industry security practices are often more tight than in other industries, and more resources are used to maintain security. This is the case in OP also.
  - Reason for this approach is the known risks targeting financial institutes. From attackers point of view bank is very tempting object. Also regulation concerning bank and insurance industry is quite strict when it comes down to security.
  - When you are working for OP please remember that you are working for a bank and insurance company.
- Technology helps to protect information, but you are one of the best protective structures and we need you to report found deviations or suspicious findings.

Thank you for being our cyber security defence!