When working from home or away from the office, it is important to understand what you must do protect yourself and our organisation against common security risks.

Here are some key reminders which you should review regularly:

*[The suggested ‘reminders’ below should be adapted to reflect your organisation’s priorities. Please delete this guiding sentence before you print & share these hand-outs with your staff.]*

|  |  |
| --- | --- |
| 1. **DO *only* use an approved device to access office systems.**
 | 1. **Do NOT use public Wi-Fi - always connect to a secure network.**
 |
| 1. **DO be vigilant of your environment - keep confidential information private (e.g. calls, conversations, all documents).**
 | 1. **Do NOT leave your computer unattended in a public place; and always lock it when unattended in private spaces.**
 |
| 1. **DO encrypt all sensitive information in transit and in situ.**
 | 1. **Do NOT forward confidential client or firm data to a personal email address.**
 |
| 1. **DO save sensitive information to the company’s central drives (never locally).**
 | 1. **Do NOT remove paper files from the office without approval.**
 |
| 1. **DO stay alert to social engineering scams and consider how you are using social media.**
 | 1. **Do NOT use the same passwords across personal and work devices and systems.**
 |
| 1. **DO report security incidents promptly to: [add details]**
 | 1. **Do NOT delay applying any software patches; and ensure security settings are set to high.**
 |
| **REMEMBER to take regular rest and stretch breaks****and keep in touch with your colleagues.** |

The above reminders provide only a summary extract of the provisions of our Remote Working Policy. Please ensure that you have read and are familiar with the current policy, available here [insert url].

Failure to adhere to the policy may lead to disciplinary action.

*This reminder sheet should be displayed in your most frequented remote working space, and one can be kept with your laptop/remote device used for work.*

FOR ANY IT ISSUES CONTACT: [Telephone/email]

When working from home or away from the office, it is important to understand what you must do protect yourself and our organisation against common security risks.

Here are some key reminders which you should review regularly:

*[The suggested ‘reminders’ below should be adapted to reflect your organisation’s priorities. Please delete this guiding sentence before you print & share these hand-outs with your staff.]*

|  |  |
| --- | --- |
| 1. **DO *only* use an approved device to access office systems.**
 | 1. **Do NOT use public Wi-Fi - always connect to a secure network.**
 |
| 1. **DO be vigilant of your environment - keep confidential information private (e.g. calls, conversations, all documents).**
 | 1. **Do NOT leave your computer unattended in a public place; and always lock it when unattended in private spaces.**
 |
| 1. **DO encrypt all sensitive information in transit and in situ.**
 | 1. **Do NOT forward confidential client or firm data to a personal email address.**
 |
| 1. **DO save sensitive information to the company’s central drives (never locally).**
 | 1. **Do NOT remove paper files from the office without approval.**
 |
| 1. **DO stay alert to social engineering scams and consider how you are using social media.**
 | 1. **Do NOT use the same passwords across personal and work devices and systems.**
 |
| 1. **DO report security incidents promptly to: [add details]**
 | 1. **Do NOT delay applying any software patches; and ensure security settings are set to high.**
 |
| **REMEMBER to take regular rest and stretch breaks****and keep in touch with your colleagues.** |

The above reminders provide only a summary extract of the provisions of our Remote Working Policy. Please ensure that you have read and are familiar with the current policy, available here [insert url].

Failure to adhere to the policy may lead to disciplinary action.

*This reminder sheet should be displayed in your most frequented remote working space, and one can be kept with your laptop/remote device used for work.*

FOR ANY IT ISSUES CONTACT: [Telephone/email]