PLATINUM
The Offshore Experts

WORKING FROM HOME SECURITY PROCEDURE

The following are the procedures we put in place to closely monitor staff productivity and activity, and prevent breach of data while staff are working from home.

A. Enhanced security measures compared to office environment:

I. Stricter monitoring of staff work time and activities

- The security software launches when the computer is turned on and is not allowed to be paused or turned off at any time during the work day.

II. Stricter monitoring of document storage protocols

- A weekly check of all staff computers will be performed and clients are expected to receive a report from the Operations Team with information on whether or not staff are compliant to the document storage policy.

III. More frequent screenshot review and reporting

- Screenshot capture of both computer monitors is enabled every 3min rather than between 3min and 9min at random.
- We review 25% to 100% of all screenshots of every staff member every day, not at random each week. The percentage will depend on how we rank them based on past use of their computer.
- The client will be sent a daily report with any violations identified and the staff member will be given real time coaching/sanction as per the VAP employee handbook.
- If no violations occur, then a weekly report will be sent to each client.

IV. Enable security software webcam feature (optional)

- We can take a photo of the staff member using the webcam every 10mins to ensure it's only the staff member at the computer and no-one else. This is optional and must be decided by each individual client in consultation with their staff to avoid any breaches of personal privacy.

V. Set parental control on Windows

- When parental control is enabled, clients can provide a specific period of time for when staff can access their PCs. With this, staff are restricted from logging in to their PCs even if they have the password throughout the blackout period nominated by the client.
- If staff needs to extend working, for example, due to power interruption within work hours, or go on overtime for an urgent task, staff can inform VAP IT or their assigned Team Leader so that the time allowed is set properly for them to continue working.

VI. Cyber Security Insurance

- Our policy covers any malicious intent committed by staff to breach client data.

VII. Activate two-factor authentication on tools/softwares

- When staff log-in to a software or a tool with their password, staff will be asked for a code as an additional layer of security. Staff will be required to verify identity using a randomised code which is generated by the company phone and is only accessible by the Admins.

VIII. Implement a Work from Home Agreement and Security Checklist

- Staff are not allowed to work from home without signing the Work from Home Agreement and Security Checklist.

B. Security measures we are continuing from when staff worked in the office:

I. Disable USB ports

- This is a standard procedure that we do to all staff PCs to prevent plugging in of external hard disks.

II. Restrict access to non-work related websites

- We restrict staff access to illegal, unethical/inappropriate sites, shopping sites and other non-work related sites to keep staff productive and stay focused on doing their tasks. Restricting these sites is also a helpful way to safeguard client data.

III. Employ a password security tool

- Passwords are easily stolen and forgotten but with the use of a password manager, the risk of getting client data compromised is prevented.

IV. Website and application monitoring

- Our security tool has capability of tracking and reporting the time spent on different websites and in different applications to help staff ensure a good use of their time and ensure that no illegal/prohibited work is being done by staff.

V. Computers to be used for work purposes only

- Our employee handbook clearly defines the unauthorised use of company computers/equipment for any non-work purposes. Non-observance to this policy are dealt with accordingly.

C. See comparison table below:

SECURITY MEASURES	IN THE OFFICE	WORK FROM HOME
Lockers (for personal belongings, mobile phones, etc.)	✓	✗
Screenshot capture	randomly between 3-9 mins	every 3 mins
Screenshot checking	10%	25% - 100%
Document storage protocol monitoring	✓	✓
WebCam photos every 10 mins (optional)	✗	✓
CCTV (optional for homebased)	✓	✓
2-factor authentication on tools/softwares (optional)	✓	✓
Enable parental control on PCs (optional)	✓	✓
Computers provided strictly for work purposes only	✓	✓
Cyber Security Insurance (includes deliberate/malicious data breach)	✓	✓
USB ports disabled	✓	✓
Restricted access to non-work-related websites	✓	✓
Password security tool	✓	✓
Website & application monitoring	✓	✓
Timetracking	✓	✓