Secure Remote Working Checklist
For COVID-19 Pandemic

Updated 19 March 2020 version 1.0

This is a risk assessment checklist designed to help those working at home on sensitive content. This should be read in conjunction the MPA Best Practices and remote working guidelines which can be viewed at www.convergentrisks.com The default policy for remote and home working is that content owners must be consulted.

If changes to key workflows (e.g., remote working) have been implemented, it is important to conduct an internal security risk assessment and any identified risks should be documented and acted upon. This checklist is intended as a guide only rather than a definitive set of procedures and technical/legal advice should be obtained in the normal way.

Where applicable, specific references to the MPA Best Practices Common Guidelines v4.06 have been provided.

No.	Clients	Completed
1.	Is the organization's client and contact database up to date?	
2.	Is each project (currently in production) appropriately mapped to a client?	
3.	Has the client/content owner provided remote working guidance and is this formally documented?	
4.	Has the organization received 'written' content owner approval for any workflow changes prior to implementation (e.g., remote/home working)? *[MS-12.6]*	

No.	Employees	Completed
5.	Has the organization documented the current number of employees working remotely?	
6.	Has the organization documented names, roles and access required (e.g., production network, corporate network etc) for all remote workers?	
7.	Has the organization provided employees with additional security awareness training covering remote working policies/processes? *[MS-4.3]*	
8.	Has the organization developed or updated its remote working policy/guidelines and disseminated these accordingly? (note: ensure policy acknowledgement is recorded) *[MS-4.x]*	
9.	Before providing employees with company owned workstations/laptops – Have the systems been hardened to the appropriate baseline guidelines? *[DS-3.8]*	

No.	Management Systems	Completed
10.	Can all organizational policies be accessed remotely (e.g., secure web-based portal or hard copy)?	
11.	Has the organization's Business Continuity and Disaster Recovery Plan been updated accordingly. *[MS-6.x]*	
12.	Have all new workflows/processes been formally documented (including all content touch points)? *[MS-8.x]*	
13.	Have all changes (policy, process and information technology changes) been reviewed and appropriately approved? *[MS-6.x]*	
14.	Have all employees and/or third-parties signed a confidentiality or non-disclosure agreement before accessing client content/information? *[MS-11.x, MS-12.x]*	

15.	Has the organization's incident management and response plan has been updated accordingly? (note: acknowledgment from all employees/third-parties must be recorded) *[MS-5.x]*	

No.	Access to production content	Completed
16.	Have all content access points (including how employees access content) been documented? *[MS-8.x]*	
17.	Is the organization tracking all content movement in and out of the production environment? *[PS-12.x, PS-17.x, DS-9.5, DS-12.x]*	
18.	Is access to client content appropriately restricted (e.g., RBAC)? *[DS-7.7]*	
19.	Is the organization implementing suitable user account management processes? *[DS-7.x, DS-8.x]*	
20.	Can employees work offline/off site (e.g., encrypted hard drives)?	
21.	Ensure all network topologies/diagrams are up to date/updated. *[DS-6.12]*	
22.	Ensure all firewall rulesets and access control lists are up to date/updated. *[DS-1.0]*	
23.	Has Secure Data Destruction policies to encompass home working been developed or updated? *[PS-16.x]*	
24.	Has the organization formalized a backup strategy for distributed content (e.g., when normal operations resume)? *[MS-6.2]*	

No.	Testing	Completed
25.	Has the organization conducted a new penetration test following key workflow changes? *[DS-1.9]*	
26.	Is the organization conducting periodical vulnerability scans (internal and external hosts and networks)? *[DS-1.8, DS-3.9]*	

No.	Physical media management	Completed
27.	Ensure all portable media dispatched from the organization has been appropriately recorded (as per shipping/receiving policy). *[PS-17.x, PS-18.x]*	
28.	Inventory all purchased and provided portable media in the organization's IT database. *[PS-12.x]*	

No.	Mobile Device Policy	Completed
29.	Implement mobile computing device security controls (if required). *[DS-10.x]*	
30.	Ensure mobile devices have been hardened to the appropriate baseline guidelines. *[DS-6.9, DS-10.x]*	
31.	Inventory all purchased and provided hardware in the organizations IT database. *[PS-12.x, DS-10.x]*	
32.	Ensure personal devices used in remote working operations are appropriately hardened (e.g., patched with latest OS release, AV/AM services running/updated, use enterprise or corporate application editions). *[DS-10.7, DS-12.4]*	
33.	Ensure two-factor authentication is implemented for accessing web-based collaboration services. *[DS-8.2.1]*	
34.	Ensure personal devices used in remote working operations authenticate with biometrics/unique passcode. *[DS-8.1, DS-10.8].*	
35.	Enforce native encryption protocols on personal devices. *[DS-10.3]*	
36.	Ensure access to web-based collaboration services utilize Corporate account information only.	
37.	Restrict personal devices to trusted networks with WPA2-PSK protocol enabled. Public wireless access points must not be used. *[DS-4.1]*	

No.	System and Security logging	Completed
38.	Log all traffic through the firewall, including remote access. *[DS-1.x, DS-7.x, DS-9.x]*	
39.	Enable logging across the internal network(s). *[DS-3.3]*	
40.	Configure and test the appropriate security alert/notifications. *[DS-9.2]*	

Convergent can provide remote assessments for home workers to verify and advise on secure home working based on the above. Our team of assessors in the US, UK and India cover most time zones. We also provide remote penetration testing in this time of increased cybersecurity risk.

For more information please contact us:

Mathew Gilliat-Smith (UK time zone)
mathew.gilliat-smith@convergentrisks.com
Office: +44 (0) 1276 415 725
Cell: +44 7715 986 893

Janice Pearson (LA time zone)
Janice@convergentrisks.com
Office: + 1 818 452 9544
Cell: + 1 323 513 6396

www.convergentrisks.com