**Information Integrity Solutions Pty Ltd**
Building trust and innovative privacy and security solutions

24-30 Wellington St, Waterloo NSW 2017 Australia

Tel: +61 2 8350 9318
Fax: +61 2 9319 5754

inquiries@iispartners.com

www.iispartners.com

# COVID-19: "The way we work"

At IIS we have always been able to work flexibly. This includes from our clients' sites, the office, the Australian Government Joint Cyber Security Centres, or our homes. This year we moved the Sydney office to the Vineyards co-working space in Waterloo with modern facilities and gigabit Internet. We have also diversified our team across Brisbane, Hong Kong, Malaysia, and Melbourne.

As the Asia-Pacific region's leading privacy and security consulting boutique we have always had a resilience mindset. We have long provided working from home (WFH) arrangements, knowing that it would make us more efficient and flexible, while allowing for work-life balance and diversity. Indeed, WFH has proven over the last few years to play to our advantage.

Companies around the world are stress testing their business continuity plans of remote working as the COVID-19 (Coronavirus) crisis is has become global pandemic.

Large to medium organisations are most likely to be well catered for remote working. They have the technology and necessary IT support to execute and have tested the capability. However, the test now will be having a larger number of staff involved, the length of the outbreak, possible impact to team morale, and various unanticipated technology, privacy and security challenges. For smaller organisations that have never worked from home and do not have a business continuity plan, the current situation may be overwhelming.

We would like to share some of our experiences to-date and provide you some tips on how we are planning to cope with the next few months – always having our team and our clients' needs front of mind.

Some of you may even see the benefits of the changes you implement now and will keep them long after the current outbreak to improve organisational resilience.

**Daily planning and forecasting**

- We empower team members to organise their daily activities and encourage them to always have a forecasting view of the next two weeks.
- We also look at other team members' calendars to coordinate work and ensure effectiveness and coordination. Most of our team members work on multiple projects and in some instances have personal commitments, so coordination is key when we are all not under the same roof, let alone the same time zone.
- End of the day check is vital to self-assess your achievements for the day.

**Flexible mind set and adaptive**

WHF requires managing family obligations and distractions. Keeping the team honest with personal or family demands and being able to adapt working hours with your manager is necessary. One size does not fit all.

**Communications**

- Better to over-communicate than under-communicate. Regular virtual stand-ups ensure all the team members are across progress, plans, issues and risks. They are also an opportunity for team bonding. As we work across time zones, we have established a daily regular check point at a suitable time for all.
- We use video and collaboration tools for internal team meetings, calls to share information, and for external client and vendor meetings.
- Smile when the camera is on! We always turn the camera on to improve communications and to be client- and team-focused. If bandwidth is an issue, quickly all switch to voice only!
- We run weekly status meetings with our clients, so we can discuss not only project progress but also possible risks and of course current challenges with COVID-19 and how we can help.

**Work from home infrastructure**

When large organisations started to roll out WFH arrangements a few years ago, the initial instructions employees needed to sign-off to were related to Occupational Health & Safety measures, forgetting in some cases the importance of security and privacy requirements.

- We have a comprehensive WFH policy where we provide our employees with comprehensive guidance on ensuring compliance with safety, privacy and security requirements.
- We all have a dedicated office space set up with stable internet connection.
- We equip our team members with the relevant ergonomic and IT equipment.

**Work-life balance**

Working in an office and running from one meeting room to another, or to an outside location helped people be more active and move sufficiently during the day. If WFH is not structured properly, people may be tempted to sit non-stop for long periods.

- We encourage regular breaks and not to skip any meals or tea breaks. We remind everyone to allow time for lunch away from their desk. Smart watches are useful for prompting breaks and opportunities to stand up and move.

- Exercise activities are also a priority and without the usual facilities available people may do less, so we encourage people to take breaks in the day to move more.
- Looking after our mindfulness and health is even more important in situations like a pandemic outbreak. We see it as a marathon, not a sprint, so establishing good habits are essential.
- We hold “Are you OK?” discussions. Each person may have different circumstances, either already isolated as they live alone, or have family members overseas that we are not sure when we will be able to see next. Having people share their experiences on calls allows for an outlet and can be an opportunity to offer advice and words of encouragement.

**Don’t forget about privacy and security**

With the wave of urgent instructions to employees to work from home, one thing we don’t want to do is lower the bar on privacy and security controls. As we have observed in previous emergencies, when organisations act hastily – including taking key controls off for the sake of short-term priorities – this raises other risks and issues.

Your organisation – and especially your employees – need to operate in a way that is mindful of the data context. For example, if you hold data that carries additional risk such as identity and other sensitive personal information, this requires further thinking and action when formulating WFH policies and access controls.

Although emergency WFH actions will not directly affect the way in which people will use or disclose personal information, it will affect the management of personal information as it will take away some physical and logical security.

IIS considers that, given the potential risks, there is a strong case for paying close attention to privacy and security risks. This is also an opportunity to do more WFH well after the current crisis is past us, facilitating better organisational resilience and diversity.

Organisations need to consider:

- Reduced probity at home vs. the organisation’s secure and limited access offices, including allowing unauthorised family or friends to view personal or business sensitive information
- Logical security controls that may impact privacy, such as weak user access management
- The implications of privacy, industry (e.g. financial services, health, energy, telco, retail) and other government legislation, policy, guidelines, etc.
- Contravention of use and disclosure requirements including the increased likelihood of data “mash-ups” on personal computers and cloud storage services
- Inadequate data loss prevention controls – if not already in place, this should be a part of user guidance on WFH arrangements (i.e. that cover OH&S, security and privacy)
- The opportunity to remind personnel in the organisation how to report a security incident or a data breach
- Staff working remotely are given access only to the personal information needed to carry out their roles and that oversight of use, including review of audit logs, is appropriate.

A useful resource is the Australian Cyber Security Centre's (ACSC) recent advice on how businesses can stay secure from cyber threats when preparing for COVID-19. In addition, the Australian Cyber Security Growth Network (AustCyber) has publish a security guide for start-ups and small business with remote working, highlighting why cybersecurity is so important in the current crisis.

IIS would also like to highlight the recent joint statement by Australian privacy regulators regarding COVID-19. They observed that privacy laws permit the exchange of critical information while also requiring personal information to be protected and to be handled in a way that is reasonably necessary to prevent and manage COVID-19. Importantly, they reiterated the value of conducting short-form Privacy Impact Assessments to help ensure personal information is handled in a way that is necessary, reasonable and proportionate.

In addition, the OAIC has developed general privacy advice for COVID-19 and guidance for Australian entities on understanding their privacy obligations to staff.

If you have questions or need help with the privacy and security dimensions of responding to COVID-19, please contact us.