Issued on 21 May 2020

ADVISORY ON COVID-19 SAFE MANAGEMENT MEASURES FOR ICT SECTOR

1. As Singapore moves to gradually ease Circuit Breaker measures, the Ministry of Trade and Industry (MTI) announced on 19 May 2020 that businesses will be allowed to resume activities in a phased manner. The Infocomm Technology (ICT) sector, except for businesses participating in retail and construction activities, will be in Phase One of the resumption of activities, and may operate from 2 June 2020.

   Please refer to MTI's **Advisory on Gradual Resumption of Business Activities in Phases Starting From 2 June 2020** issued on 19 May 2020 for more information.

2. Businesses in Phase One need not apply for exemption before resuming operations. MTI will grant these businesses a class exemption to resume business. Businesses must submit their manpower details via the GoBusiness portal within two weeks of resuming operations, and must also comply with the requirements for safe management measures.

3. The Ministry of Manpower (MOM) has laid out the safe management measures and requirements that employers and businesses will need to put in place to resume operations at workplaces. The requirements fall under six categories:
   A. Implement system of safe management measures at workplaces;
   B. Reduce physical interaction and ensuring safe distancing at workplaces;
   C. Support contact tracing;
   D. Require personal protective equipment and personal hygiene;
   E. Ensure cleanliness of workplace premises; and
   F. Implement health checks and protocols to manage potential cases.

   Refer to MOM's advisory on **Requirements for Safe Management Measures at the workplace after Circuit Breaker period**, issued on 9 May and updated as of 16 May 2020, for more information.

4. **All employers and businesses, including those in the ICT sector, must comply with the MTI and MOM nation-wide advisories in all workplaces and workplace settings.**

5. In this document, the Infocomm Media Development Authority (IMDA) and SGTech have set out additional measures for certain workplace settings specific to the ICT sector. The workplace settings included in this document are:
   I. Providing onsite IT services, support or manpower at customers' premises;
   II. Data centre operations; and
   III. ICT retail stores and e-commerce.

6. **Employers and businesses that have operations applicable to these workplace settings must comply, not only with the measures set up by MTI and MOM, but also with the following additional measures where applicable.**

I. PROVIDING ONSITE IT SERVICES, SUPPORT OR MANPOWER AT CUSTOMERS' PREMISES

7. As far as possible, minimise physical meetings, onsite work and provide support and services remotely (e.g. over the phone, teleconference). Measures to enable this could include reviewing the work processes, providing the necessary IT equipment and adopting solutions that enable remote working and IT support.

8. Employees visiting or working at customers' premises must comply with the customer site's safe management requirements (e.g. temperature taking, protective equipment and personal hygiene, maintaining a safe physical distance, reduce and limit physical interactions).

9. Employees must wear masks and maintain at least 1-metre safe distancing at all times.

10. Brief employees on higher risk sites or locations, so that employees can take extra precautions and measures (e.g., hospitals, Government Quarantine Facilities (GQFs), foreign employee dormitories).

11. Where possible, assign dedicated support teams to customers, or groups of customers, to perform such services. There should not be cross deployment and interaction of teams or members servicing different customers or customer groups. If cross-deployment cannot be avoided (e.g. insufficient employees with required skills), additional safeguards must be taken to minimise the risk of cross infection (e.g. systems are in place to ensure no direct contact with the cross-deployed personnel) and put in place split teams for business continuity.

12. For businesses using outsourced suppliers or contractors, the same safe management measures and practices must be implemented by these outsourced parties. Interactions amongst all parties (employees, suppliers, customers, etc.) should be kept to a minimum and duration of interaction should be as short as possible. Implement staggered work or scheduling to prevent different teams from mixing.

13. As far as possible, do not share machinery, tools or equipment across staff, teams or customers. If there are no options (e.g. public kiosks, specialized equipment, etc.) please ensure that these are regularly cleaned and disinfected before changing hands. The sanitation and hygiene advisories disseminated by the National Environmental Agency (NEA) must be adhered to.

14. Keep records of employees and service providers, on shift and duty roster, and the customers and locations visited.

II. DATA CENTRE OPERATIONS

15. Data centres have additional requirements as the daily operations typically includes the following:

    (i) Extended access by specialized personnel and multiple parties – such as employees, vendors and contractors, facilities management, tenants and customers;

(ii) Being conducted in dedicated, co-located/multi-tenanted, or part of multi-use facilities (e.g. in the case of smaller data centres, server rooms or companies such as banks hosting their own operations); and

(iii) Varied activities onsite, such as expanding rack-space, fitting-out works and IT services.

16. As far as possible, data centre operators should minimise onsite work. Measures include:

(i) Reviewing the work processes, providing the necessary IT equipment and adopting solutions that enable remote access to the equipment, such as VPN access to building management systems for remote data centre monitoring, SOPs to allow for remote co-piloting;

(ii) Requiring functions or activities that do not need access to specialized equipment to be conducted from home, such as: business development & strategy, administrative functions (e.g. Human Resources, Finance), procurement & sourcing, sales & marketing;

(iii) Informing customers of the technologies available that would allow them to manage their workloads remotely and suggesting to customers to test their ability to respond to events remotely before it becomes necessary to go on site; and

(iv) Postponing all non-essential maintenance and projects.

17. Operators should coordinate safe management measures among all companies involved in the data centre operations (e.g. with third-party facility management and other outsourced services) to ensure that staff are not confused by conflicting requirements and policies.

18. Interactions amongst all parties (employees, suppliers, customers, etc.) should be kept to a minimum and duration of such interaction should be as short as possible.

19. Plan for redundant operations by creating teams of mission-critical staff, with each team comprising members that have a mix of skills/experience who can effectively manage the facility. This plan should also include team segregation between sites, and having different teams working in separate workspaces. Team members should also continue to work in the same shift to avoid cross-shift contact.

20. For work that is usually carried out by different groups, specialists or suppliers:

(i) Implement staggered work hours or scheduling of different activities (e.g. maintenance, testing and commissioning, fitting-out work) to prevent mingling of different teams or companies;

(ii) Where possible, there should be no cross deployment of employees to different teams. If cross-deployment cannot be avoided (e.g. insufficient employees with required skills), additional safeguards must be taken to minimise the risk of cross infection (e.g. systems are in place to ensure no direct contact with the cross-deployed personnel);

(iii) Where possible, the staggered or split team arrangement should be consistent or extended to other suppliers or teams along the chain of activities, e.g. Team A should only be working with Team A from a supplier.

21. The frequency of cleaning and disinfection (as reasonably practicable as possible) for all common spaces should be increased, and all machinery and equipment that the on-site personnel have interacted with to be cleaned or disinfected once per every shift or team change. Ensure that machinery and equipment shared between personnel across different teams, customers or service providers, are cleaned and disinfected before changing hands. The sanitation and hygiene advisories disseminated by the National Environmental Agency (NEA) must be adhered to.

22. For on-site construction projects that entail major upgrades or extensions of capacity:

(i) Organisations involved should suspend all non-essential projects where possible;

(ii) If the project must continue, organisations will need to coordinate with contractors to ensure all safe management measures are adopted by the subcontractors/vendors;

(iii) Where possible, a separate secure entrance for contractors and vendors should be setup;

(iv) Construction project team members should not interact with the data centre operations team members; and

(v) Construction work activities should also adhere to prevailing MOM, MOH and BCA advisories on this topic.

23. Only allow scheduled employees and visitors into the data centre. Eliminate all unnecessary access and visits for customers and vendors.

III. ICT RETAIL STORES AND E-COMMERCE

24. Companies should comply with prevailing safe management measures issued by ESG for retail establishments and online retail delivery.

ADDITIONAL RESOURCES

25. Please refer to PDPC's advisory for personal data protection measures to consider when implementing safe management measures and solutions.

26. For companies looking for remote working and safe management solutions, refer to IMDA's compiled list of digital solutions and resources.

For queries and feedback, please contact **IMDA** at info@imda.gov.sg and **SGTech** at info@sgtech.org.sg