UNITED ARAB EMIRATES الإمـارات الـعـربية المتحدة

الـمـجـلـس الأعـلـى للأمن الـوطـني

THE SUPREME COUNCIL FOR NATIONAL SECURITY

الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث

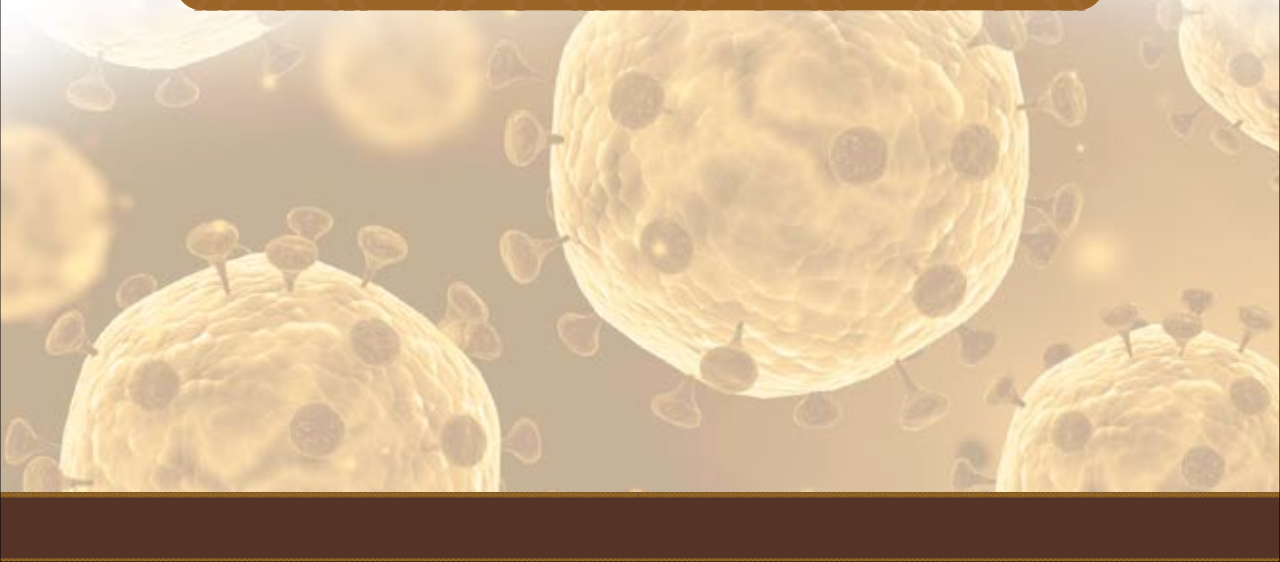
National Emergency Crisis and Disasters Management Authority

# Business Continuity Readiness Guidelines for UAE Organizations

## In the event of the Novel Coronavirus (COVID-19)

AE/SCNS/NCEMA 7002:2020

Version (I)
March 2020



## Contents

Contents

## 1.0 Introduction

This Guide is a guiding document to increase the readiness of the organizations in the UAE and maintain the provision of the essential services and products, as well as to reinforce the importance of synergy and sustainable cooperation between all concerned organizations in the UAE.

This Guide explains ways to address the risks arising from the outbreak of epidemics in the organizations that may directly affect business continuity and community stability. In case the new COVID19- virus spreads among employees at the workplace, precautionary and preventive measures should be taken to ensure the general safety of the employees.

UAE organizations at federal, local and private levels shall adopt this approach by assessing risks, threats, weaknesses and consequences thereof, where the organizations concerned may adapt their approach to identifying risks according to nature of work.

Scenarios, assumptions and considerations were developed in an integrated manner to guide the process of planning at all levels, as related to points of improvement and the potential impacts of risks and threats.Business impact analysis is necessary to quantify the capabilities in terms of quantity and efficiency to perform the tasks. These capabilities should reflect in emergency and crisis plans, as well as in business continuity (in the short term for the emergency, crisis and disaster cycle) and in national preparedness strategies (in the long term).

Preparing for any event is the responsibility of all organizations and levels (federal, local and also the private sector) and it is also the key to success in managing any emergency or crisis case. Preparation exercises can be conducted prior to incidents. The organizations may also involve all partners from governmental and private organizations and society. The national preparedness and readiness course for prevention, response and recovery tasks can be summarized as follows:

- Plan
- Organization & Staff
- Preparation
- Training
- Excercises, evaluation, and Continuous Development

## 2.0 Concepts

| | |
|---|---|
| Business Continuity | The ability of the organization to continue its prioritized activities at predetermined level after the occurrence of disruptive incident. |
| Business Continuity Plan | Set of procedures in a documented form, which direct the organization to react, recover, restore and restart the predetermined level of operations after the interruption. |
| Epidemic | Health emergency that is represented in the emergence of cases of a severe disease among a group of people in a specific geographical area during a specific period of time with an obvious increase from the normally expected number compared to a similar period in the previous period, in the same location and time, for the same region, thus causing concern at the national level. |
| Sick Person | A person who is afflicted with the sickening factor, its toxic products or secretions, whether or not the signs and symptoms of the disease appear on him/her. |
| Contact Person | Any person who has been in contact with a sick person or a carrier of the sickening factor in a way that the infection is likely to be transmitted during the period of the disease spread. |
| Quarantine | Restricting the activities of healthy people or animals who were exposed to the sickening factor during the period of disease spread, for a period equivalent to the longest incubator period. |
| Sanitary Isolation | Separating the sick person, or a person suspected of being infected, from other healthy people, voluntarily or shortly, for the duration of the disease infection in appropriate places and health conditions, in order to prevent the transmission of the infection from the sick person or the person suspected of being sick to others. |
| Employees / Staff | Individuals working within the organization at all levels. |
| Customers | Individuals and customers from outside the organization of the concerned parties. |

## 3.0 Purpose

The purpose of this Guide is to demonstrate precautionary and preventive measures aiming to sustain business continuity for organizations, through:

- Protecting and safeguarding individuals and society from the risk of epidemics in organizations.
- Determining the critical functions for business continuity measures, taking into account the potential impacts of the epidemic.
- Knowing the necessary measures to be taken in the event of an epidemic outbreaks among employees.
- How to activate business continuity plans in the event of losing individuals due to an outbreak in the workplace.
- Reducing and minimizing the spread of the epidemic in the organization.

## 4.0 Assumptions and considerations

Through reviewing the specialized studies on the prevalence of epidemiological cases, assumptions and considerations have been developed that help reaching a comprehensive understanding of planning for business continuity in the organizations, as indicated below:

- Spread of rumours, impacting the reputation of the organization and spreading panic among the employees.
- Outbreak in an organization or any of its facilities.
- identifying a sick person or contact(s) with sick person(s).
- Difficulty in controlling the spread of the epidemic in the organization.
- Absence of vaccine or medicine to limit the spread of the epidemic in the organization.
- Intense presence of individuals in the workplace.
- Providing essential services and products.

## 5.0 Setting Priorities

Work priorities are set for the key elements as criteria to ensure business continuity; which are the individuals, systems and critical locations in the organization and the mechanism of accessing them:

- Identifying the critical functions.
- Determining the parties concerned with dependability in business continuity.
- Determining alternative places or locations that could be used to perform business in the event the main site is affected by the epidemic.
- Using technology to serve business continuity, e.g. remote work, electronic transformation and artificial intelligence.
- Establishing preventive measures for the organization to avoid being affected by the epidemic or for early detection of suspected cases.
- Securing supply chains that would affect business continuity in the organization.

## 6.0 Preventive and Precautionary Measures

The following points are considered as controls for the preventive and precautionary measures that organizations must follow in order to ensure the safety and protection of the work environment. The procedures are divided into three categories, as shown in the figure below:

### 6.1 Preventive Measures:

- It is mandatory to follow the guidelines issued by the Ministry of Health, Community Protection and the relevant health authorities.
- Ensuring that disinfection and sterilization operations are carried out through the implementation of standards, instructions and requirements issued by the competent authorities
- Ensuring the availability of the appropriate health requirements, according to the nature of the organizations work.

- Determining and specifying temporary places for sanitary isolation (for organizations that have large numbers of employees and residential complexes).
- Defining the medical and logistical requirements in coordination with the concerned authorities.
- Raising the efficiency of the individuals involved in the security and protection of the organizations to ensure proper handling of any situation or suspicion of a situation.
- Preparing work teams and carrying out periodic exercises to check teams' readiness.

## 6.2 Preparedness and Increasing of Readiness:

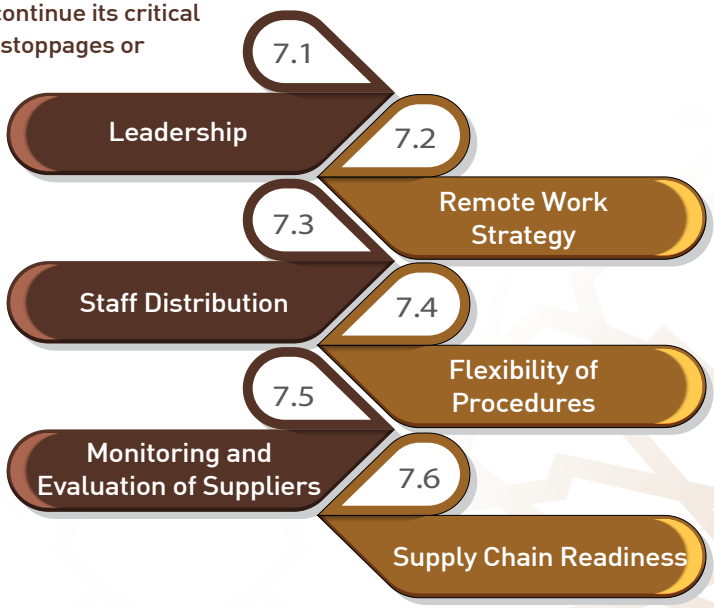
- Monitoring employees' health status by tracking the status of employee vacations for the past and upcoming period and their travel destinations for official tasks or for personal purposes.
- Providing thermal detection devices for organizations that receive large numbers of customers.
- Coordination and prior identification of the hospitals concerned to transfer the suspected cases (after isolation).

## 6.3 Response and Handling of Cases:

- Isolation of suspects in places designated for temporary isolation (pending transfer to hospital).
- Determining the contacts of confirmed and suspected cases.
- Coordination with health organizations to transport contacts to hospitals to carry out the necessary checks.
- Providing the necessary logistical support in all cases.

## 7.0 Planning for Business Continuity During Outbreaks

**Business continuity planning stage is based on major steps that depend on the effectiveness and ability of the organization to continue its critical activities in the event of business stoppages or disruption:**




### 7.1 Leadership:

- Activating the procedures necessary to respond to the event during epidemics.
- Directing and supporting security and protection programs with the necessary resources and following up to ensure that their objectives are achieved.
- Supporting and providing the necessary resources, needs and requirements to implement the business continuity plan and mitigate the risks associated with the disruption of operations.
- Coordination with external parties (police, transport, ambulance, and hospitals) to request support and assistance.

### 7.2 Remote Work Strategy:

- Readiness of the technical infrastructure of the organizations to work remotely.
- Readiness of the employees to use the Technology of remote work.
- Ability to manage the systems internally or remotely.
- Determining and classifying the jobs that must be available in the workplace and the jobs that can be continued with the remote work.

- Providing health control and preventive measures for public safety.
- Monitoring the efficiency of remote work performance.
- Determining other alternative facilities or sites for carrying out the critical functions.
- Possibility of outsourcing the implementation of Critical activities according to the nature of work in the organization.

## 7.3 Staff Distribution:

- Determining the number of employees for critical jobs and distributing them in different locations in order to reduce mixing and contact.
- Determining the number of employees for less critical jobs and using remote work technology to reduce mixing and contact.
- Developing a policy or a procedures for immediate employment and completing any shortage in the workforce, if any.

## 7.4 Flexibility of Procedures:

- Setting a mechanism for the attendance of employees by the flexible hours and sick leave system.
- Giving authority to directors or line officials in remote centres to dismiss employees from their workplace to reduce staff density to prevent mixing and contact.

## 7.5 Monitoring and Evaluation of Suppliers:

- Setting a mechanism for monitoring the suppliers and the system of their attendance in the organization.
- Evaluating suppliers and verifying the controls applied to them.
- Ensuring that all resources are provided when needed by suppliers and service providers as per the concluded contracts and agreements.

## 7.6 Supply Chain Readiness:

- Focus on supply chain management and supply network construction for service requirements.
- Coordination of activities with supply chains to ensure business continuity for the requirements of the organization.

## 8.0 Indicators of Remote Work Efficiency

- Employees' familiarity with how to use the technology of remote work.
- Mechanism to monitor employees' attendance and leave remotely.
- Electronic systems or procedures that enable activating means of communication and holding meetings remotely.
- Monitoring the status of tasks accomplished remotely.
- Daily reports of the level of work productivity.

## 9.0 Preparedness and Readiness Measurement Tools

### 9.1 Institutional Readiness form

| Institutional Readiness | | |
|---|---|---|
| Procedures | | |
| Remote Work Readiness Verification | | |
| Notes | Employees | Yes/No |
| | Employees' familiarity with the required procedures upon readiness verification | |
| | Employees have already been involved in courses / exercises during which remote work technique has been activated | |
| | Do employees use technology to work remotely during normal situations? | |
| | The presence of technology and technical means for employees to do the work remotely (laptops, smart phones, tablets, etc.) | |
| | Have processes, vital functions and personnel in charge for them been identified? | |
| Technology (infrastructure, hardware, software, knowledge) | | |
| | Availability of remote computer-connection systems; (VPN), (Remote Desktop), etc. | |
| | Existence of a sufficient number of licenses for the remote work system as required for all concerned employees | |
| | Staff familiarity with the required technology when activation | |
| | Have the employees been introduced to these systems? | |
| | Existence of a written user guide / video on how to use the required technology | |
| | Possibility of using remote systems (system management) | |
| | Availability of a mechanism through which the attendance of employees can be recorded remotely | |
| | Existence of systems for holding meetings remotely | |
| | In case of power outages, the existence of a mechanism to restart equipment automatically | |
| | Staff can receive technical support remotely | |

| | | |
|---|---|---|
| | Does the data center exist outside the organization? | |
| | Is the data center managed by a third party? | |
| **Customer Service (if applicable)** | | |
| | Customers can receive the required services through smart platforms | |
| | The organization's smart services are ready and available to the public through websites or applications | |
| | Can all services be %100 automated for customers within one week, if they are not all ready? | |
| **Examine preventive and precautionary measures** | | |
| **Logistics Services** | | |
| | Are the facilities inside the institution sterilized as per the procedures set by the health authorities? | |
| | Is there a mechanism in place to clarify the health status of employees in the operational and service providers' companies? | |
| | Are there alternatives to contracts with operational and service providers? | |
| | Are the organization's transportation means (if any) sterilized as per the procedures set by health authorities? | |
| | Existence of places for temporary sanitary isolation if the need arises | |
| | Possibility of providing the necessary logistical support in all cases | |
| **Preventive Measures** | | |
| | Have preventive measures been put in place to monitor suspected cases in cooperation with the relevant authorities? | |
| | Have public safety preventive measures been put in place according to the guidelines document for agencies and institutions to deal with the developments of the new Coronavirus 2019? | |
| | Have the preventive measures issued by the health authorities been circulated to the employees? | |
| | Are all employees familiar with preventive measures? | |
| | Activities of high and intense contact are suspended or cancelled | |
| | Involvement of the authorities in the process of monitoring, following up and reporting on the health status of the employees | |
| | Have the individuals concerned with the security and protection of the organizations been trained to ensure proper handling of any situation or suspicion? | |
| | Has coordination been made with specific hospitals in order to transfer the suspected cases (after isolation)? | |
| | Do all the employees in the organization have valid health insurance? | |

## Contact

**For additional information, please contact National Emergency, Crisis and Disaster Management Authority:**
**Safety and Prevention Department, Business Continuity Section:**
**Phone: 024199499 ,024177073 ,024177154**
**Email: bcm@ncema.gov.ae , Website www.ncema.ae**

## 9.2 Readiness of employees for remote work form

| No | Name of Activity / Service | Activity Criticality Category | Total Staff | No of employees required to work from the workplace | No of employees for remote work | Remote work readiness | electronic system availability | Other requirement for remote work | Remarks |
|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | | | | | | |
| 2 | | | | | | | | | |
| 3 | | | | | | | | | |
| 4 | | | | | | | | | |
| 5 | | | | | | | | | |

| Criticality category level | Criticality or risks level |
|---|---|
| Level 1 | It must be recovered in less than 8 hours |
| Level 2 | It must be recovered within 24-8 hours |
| Level 3 | Minimum impact or risk, required within one or two days |
| Level 4 | Medium term required within one week |
| Level 5 | Medium term required within two week |

## 10. References

Federal Law No. (2014/14) on Combating Communicable Diseases.

Business Continuity Management Standard AE/SCNS/NCEMA 7000

## Disclaimer

## Appendix A
# Remote Information access procedures

These procedures were prepared in alignment with the future vision of the National Data Authority (NDA), which seeks to achieve the basic pillars of data protection in the UAE. NDA is the future data arbitrator and the major operator of cloud services for all the relevant governmental data. The following procedures are binding on all the services provided by service providers including distance education, working remotely (as described in clause 7.2: Remote work strategy), and any other services that facilitate remote access to information.

The use of the various remote information access services through the network by the service providers and companies contracted to provide the service of remote information access, must comply with the data protection law No. (34) for the year 2019 and all the relevant legislation in this regard. In addition to following the best practices and standards in accessing, using, and analyzing the information accessed remotely. Therefore, service providers and users are obligated to the following as regulatory procedures in regard to the remote information access initiative:

1. The concerned authorities are obliged to implement the policies and standards of the Data Protection Law No. (34) for 2019 and must ensure that they are implemented in accordance with the regulations and decisions issued by the authority, including their ownership of all data and not the provider.
2. The concerned authorities are obliged to be compliant with the information security policy and standards to ensure information security in this regard which is issued by the Signal Intelligence Agency (SIA) (formerly the National Electronic Security Authority - NESA) taking into account the regulatory framework for competition from the Telecommunications Regulatory Authority (TRA) (www.tra.gov.ae/assets/sC5ggLz7.pdf.aspx ) and align it with the government agencies application standards.
3. The concerned authorities must be complied with the standards and policies adopted and applied by the Telecommunications Regulatory Authority (TRA) to enhance cybersecurity in correspondence with the regulation and classification of data protection for cloud computing in the UAE (https://www.tra.gov.ae/userfiles/assets/vzjmlB3CM34.pdf).
4. The concerned authorities must adhere to apply the security and legal requirements and legislation in place concerning Data storage and Data retention, provided that the minimum storage period is one year for the Data content, and two years for metadata.

5 The concerned authorities applying the technologies of the remote information access must ensure the security of their internal networks and the security of remote communication of information.

6 The concerned authorities should monitor the remote information access activities and adhere to the principle of need-to-know and limit the access to information and applications that are needed for work purposes.

7 The authorities applying the technology of the remote information access are not allowed nor are characterized by the legal right to perform any mean of data processing on their own data without the approval of the National Data Authority. Accordingly, if the application of remote information access technologies are for the purpose of data processing and analysis, the processor must adhere to the extracted and specific conditions as follows:

- ✓ Processing the data in accordance with legally legitimate cases with the application of the above-mentioned law (Data protection law) and the instructions issued by who is of a quality, and that the purposes and practices of the analysis are legitimate and does not violate public order or public morals.
- ✓ Adherence to the period of processing the data and not exceeding its purpose with notifying the authorized authority, to be delivered and wiped on the agreed time lapse.
- ✓ Not to disclose data except in legally authorized cases, while ensuring its protection and security in accordance with the legislation in place on this regard.
- ✓ Not to cause harm to the data owner's against the purpose of the analysis.
- ✓ Create a detailed data record.
- ✓ Providing what is necessary to prove the application of the requirements of these procedures or the Data Protection Law No. (34) for the year 2019 to the owner of the data.
- ✓ Obtain the prior approval of the National Data Authority to analyze, process, and use the data.
- ✓ For all data is to be hosted and stored within the UAE, alongside with its backups.