UNOPS

Headquarters, Copenhagen
3 Avril 2018

EXECUTIVE OFFICE INSTRUCTION REF. EOI.ED.2018.03

BUSINESS CONTINUITY PLANNING

1. Authority

1.1. This Executive Office Instruction (EOI) is promulgated by the Executive Director UNOPS, under the EOD.ED.2017.02 – Organisational Principles and Governance Model.

2. Purpose

2.1. This EOI establishes the Business Continuity Planning (BCP) for UNOPS globally.

2.2. Its purpose is to mitigate the risk in the event of a disaster in a UNOPS office by providing a framework of procedures, organisational structures, and preparedness measures to preserve the continuity of critical/essential services and functions, and liaison and coordination with national authorities, the UN system and other stakeholders.

2.3. The specific processes underpinning the management of UNOPS BCP, as well as the proposed template and additional instructions shall be included in the Process and Quality Management System (PQMS).

3. Effective Date

3.1. This EOI shall become effective **immediately**.

4. Consequential Changes

4.1. This EOI shall supersede and replace Administrative Instruction AI/CSG/2010/01 No.15, dated 1 April 2010 and any associated addendums.

[signature redacted]

Grete Faremo
Executive Director, UNOPS

UNOPS

EXECUTIVE OFFICE INSTRUCTION Ref. EOI.ED.2018.03

BUSINESS CONTINUITY PLANNING

TABLE OF CONTENTS

1. Definition

1.1. UNOPS recognises the potential strategic, operational and financial support risks associated with service interruptions. The capability to respond effectively and maintain critical business processes is essential to UNOPS operational mandate and to maintaining credibility with partners and stakeholders. Business continuity planning encompasses all the information and processes required for UNOPS to achieve those objectives.

2. Objectives

2.1. The objective of this EOI is to establish the basic principles necessary to ensure emergency response, resumption and recovery, restoration and permanent recovery of UNOPS operations and activities during a business interruption event.

2.2. This EOI also provides guidelines for developing, maintaining and exercising regional and country specific business continuity plans.

2.3. This EOI applies to all UNOPS personnel, facilities, infrastructure and IT systems at all UNOPS offices, throughout the world. UNOPS offices shall be prepared for scenarios for any unplanned event, occurrence or sequence of events that has a specific undesirable consequence. This includes but is not limited to, political instability, natural disaster, disease outbreak, power outage, ICT failures, data corruption, explosives and chemical, biological and nuclear hazard.

2.4 These events may be localized, rendering only a single office facility inaccessible, or could have regional impact, with multiple offices facilities in a geographic region becoming inaccessible.

3. UNOPS Headquarters (HQ) BCP

3.1 The Shared Services Center (SSC) shall coordinate the development of the Business Continuity Plan for HQ. However, recognizing that HQ BCP has ICT content, the actual development of the plan shall be initiated by SSC and fully supported by ICT.

3.2 HQ units as determined by SSC must maintain their own supplementary BCPs that will be integrated as Annexes into the HQ BCP. All unit supplementary BCPs that rely on IT systems should be reviewed by ICT.

3.3 UNOPS wide IT systems and services shall be addressed in the ICT annex to the HQ BCP.

4. UNOPS Regional and Country BCPs

4.1. UNOPS Regional Directors have the responsibility and accountability to ensure that BCPs are prepared in their respective regions. They are also responsible for ensuring that the processes are in place for the training, testing and implementation of the BCPs as required.

4.2. BCPs for Regional Offices shall be developed by the Regional Office and are the responsibility of the Regional Director.

4.3. Other BCPs shall be developed by the respective Hub and OC Director, Project Centre Managers, Project Manager and others who are the senior most UNOPS personnel in country.

4.4. The Head of Office/senior most person responsible to develop a BCP is the “Plan Owner”.

4.5. The UNOPS Chief of Security, in close cooperation with the SSC, will coordinate the creation and revision of the regional and country BCPs, to ensure appropriate consistency, coordination and compliance with this EOI.

5. Content

5.1. A BCP is intended to serve both as a work plan for achieving readiness and as a guidance tool for response during a disaster.

5.2. Each UNOPS office is required to have a comprehensive BCP. The objectives of the BCP should consider the following:

- Safety of personnel.
- Minimize damage and losses and eliminate or mitigate the impact of disruptions on operations.
- Ensure continuation of critical processes and critical operational services.
- Achieve a timely and orderly recovery across a wide range of potential hazards that could affect all operations, security and/or ICT with subsequent reconstitution of normal operations that allows the resumption of critical processes and operational services.
- Ensure the succession of management in the event of a crisis situation.
- Liaison and coordination with local authorities, United Nations system and other stakeholders.
- Protect and ensure access to essential facilities, equipment, vital records and assets.

- Provide organisational and operational stability, by having the capacity to continue and control critical processes, operational services and functions until normal activities are reconstituted.
- Facilitate decision-making during an emergency or crisis event.

5.3. Accordingly, a BCP for each office should:

- Lay out the steps to ensure the capabilities are in place to continue essential operations in the event of an emergency or when exposed to a broad range of risks.
- Define the roles and responsibilities of UNOPS personnel and specific actions to be taken by the office to ensure continuity.
- Maintain current lists of all ‘critical’ personnel.
- Maintain detailed plans to secure priority assets, documents, and information.
- Include key security aspects, including but not limited to: UNOPS safety and security policies and instructions; procedures and specific in-country security procedures and alignment to the UN Country Security Plan established by the UN Security Management System (UNSMS).
- Contain mandatory instructions, procedures and guidance concerning internal and external communications.
- Include technical measures that enable the recovery of information technology systems, operations, and data that is identified as critical.

- Be based on a risk assessment that considers potential losses due to unavailability of service versus the cost of resumption, anticipating a variety of probable scenarios.

5.4. The BCP should also reflect that following a disaster, the reconstitution of offices and personnel to restore complete functions is a priority. Reconstitution operations may include actions to restore the primary warehouse facility to operational capability, or acquiring a new facility, working closely with other UNOPS, United Nations offices and the respective Government, acquiring and installing equipment and communications, and redeploying personnel to the alternate site. Reconstitution sites may include other offices or those of other UN agencies.

5.5. The eventual establishment of an emergency relocation site at time of crisis, as is appropriate should be done in consultation with ~~the Deputy Executive Director~~ the Chief Financial Officer/Director of Administration, the Director, Regional Portfolios, [REV. 05.05.2020] the SSC, the respective Regional Director and UNOPS Chief of Security.

5.6. In most cases, it may not be necessary to redeploy personnel to another location. To address local crisis situations, alternate approaches for resumption including remote working from home may be identified.

6. Testing and Updating

6.1. BCPs should be tested at least annually to ensure recovery preparedness. The scope, objectives and measurement criteria of the tests shall be determined by the head of office/plan owner.

6.2. BCPs must be updated when there are changes in personnel responsibilities, contact information or functional changes. A review of the BCP must be done regularly to ensure that the information in the plan is up to date and correct. Substantial changes to the BCP must be signed off by the Plan Owner/Head of Office and shared with the UNOPS Chief of Security and SSC.

6.3. The Plan Owner/Head of Office is responsible and shall be held accountable for ensuring that parts of the plans are tested annually and that they are updated as outlined in paragraphs 6.1. and 6.2.

7. Corporate Communications

7.1. External communication during time of crisis is a critical business process. SSC shall work with the Communication Unit to develop both internal and external communications in the event of a business interruption.

8. Training

8.1. UNOPS offices shall ensure that all personnel are made aware of their responsibilities under their respective BCPs.