EUROBANK S.A.
8, Othonos Str., GR 105 57 Athens
GCR: 154558160000
Tel.: (+30) 210 333 7000
eurobank.gr

April 2020

Eurobank S.A. - Business Continuity Statement

Eurobank S.A. has long recognized that a wide variety of disruptive events or unforeseen circumstances can cause significant disruptions to its business operations.

The Bank is committed in mitigating this risk of business disruption in order to preserve its reputation, safeguard revenues, serve its clients and sustain both a stable financial market and customer confidence.

Therefore the Bank has adopted a solid Business Continuity Management System (BCMS) in order not only to provide effective response to a wide variety of disruptive events, but also to minimize their impact on the Bank's smooth and proper operation. More specifically, the BCMS is based on predefined strategies and risk assessment methodologies, is designed to identify risks, assess their impact and safeguard the continuation of critical business processes & systems.
Eurobank's S.A. BCMS has been formed under the requirements of the Central Bank of Greece at national level and is also certified with the international standards ISO 22301:2012 by TUV Hellas since 2013.

Key elements of the BCMS are:

A. Business Impact Analysis
The identification of risks & critical business functions is accomplished, through a Risk Assessment Methodology.

B. BC Plan development
As part of the BC Plans,
(a) Critical services provided to the clients are acknowledged
(b) Minimum resources needed for the continuation of critical services are defined. The identified resources are not restricted to human & IT, but also include the identification of critical flows of information, within and outside the Bank & critical physical and electronic documents.

C. Business Continuity Recovery Solutions

➔ **Alternative Sites**
In the event of a BC incident, Business units have plans that include relocation to, self-managed, dedicated standby facility. This recovery site is physically separated from the primary site to prevent both from being affected by the same incident. Moreover, an IT alternative site exists, that provides the necessary infrastructure and critical systems on a hot standby basis.

➔ **Diverse Locations**
Some business entities occupy more than one office locations, in different building facilities. In the event of a BC incident, at one office location, the business activities

are transferred to the other ones, at which staff and facilities are already prepared to handle them. These diverse locations are geographically separated.

➔ **Reciprocal Agreements**
Some business entities have agreements with other business units regarding the allocation of a required number of recovery seats. The production sites of both business units are physically separated from each other to prevent both sites from being affected by the same incident.

➔ **Remote Access**
Staff has the ability to work remotely even from home in a secure manner and use all systems and tools necessary to support daily work tasks. This type of recovery solution is suited for the continuation of paperless critical business functions, while ensuring at the same time that operations performed off-premise are qualified with a system of internal controls equivalent to that running when these are performed on premise.

D. BC Plan Maintenance
BC Plans are reviewed, updated and tested at regular intervals, as well as after significant changes to existing operations and/or capabilities.

E. BCMS Teams
Roles are assigned across all organizational levels, from Top Management to Business Unit level. Indicatively, BCMS Teams at Top Management level are:
- ✓ Reviewing BCMS performance annually
- ✓ Deciding on improving coverage
- ✓ Handling BCP crisis

On the other hand, BCP Teams on Business Unit level are:
- ✓ Performing risk assessment & identifying critical business processes
- ✓ Developing, testing & updating BC plans
- ✓ Activating BC Plans, in case of disruption etc.

F. Third Party Services
All our Critical Service Providers are contractually obliged to have Business Continuity plans in place to safeguard the proper performance of the services, if the ordinary operation of the Service Provider is disrupted.

G. Audit
BCMS is subject to:
(A) an annual internal audit
(B) periodic review by the Central Bank of Greece
(C) an annual audit by TUV Hellas

More details on the BCMS cannot be provided in this notice, as the Bank keeps them confidential, in order to safeguard their effectiveness & security.

Penny Maniati	Ioannis Tzanos
Group Organization & Business Analysis Sector	Group Corporate Security Officer