Veles International

BUSINESS CONTINUITY POLICY

November 2019 revision

Objectives of the BCP

This Business Continuity Policy ('*this Policy*' or the 'BCP') has been developed and is permanently maintained by Veles International Limited ('*VIL*') to ensure that it is able

I. to continuously deliver its services to the satisfaction of its clients without damaging their interests;

II. to continuously communicate with the competent authorities, provide necessary reports, respond to queries and support investigations.

It's vitally important to protect VIL's business from the unexpected. Whether this is from power cuts, IT system or equipment failure or natural disaster, VIL strives to make sure its business is not vulnerable to disruption (outage) and it can recover as quickly as possible. VIL's Board of Directors (the 'BoD') recognizes that the disaster can strike the organization at any time. VIL, therefore, needs to have a process in place that ensures the operation is able to mitigate the impact and return to "business as usual" in the shortest time possible.

For these purposes the following is taken into account:

- *Context of VIL* - the environment in which it operates including internal and external factors that can have an effect on its business continuity plans;
- *Interested Parties, or Stakeholders* - persons or organizations that can affect, be affected by, or perceive themselves to be affected by VIL's activity;
- *Minimum Business Continuity Objective ('MBCO')* - the minimum level of VIL's services and products that is acceptable to VIL to achieve its business objectives during a disruption, that is to provide services to its clients;
- *Maximum tolerable period of disruption ('MTPD')* - the time it would take for adverse impacts of the complete outage to become unacceptable;
- *Prioritized timeframes* - order and timing of recovery for critical activities. Warning and communication activities undertaken during an incident.

The BCP is designed in accordance with

- Section 17(4) of the Law 87(I)/2017 ('*the Law*') which transposes into Cyprus law the Directive 2014/65/EU of the European Parliament and of the Council ('*MiFID II*');
- ISO 22301 Business Continuity Management (as appropriate to the scale and specifics of VIL's business, as well as the context of VIL);
- existing best practice that may be relevant to VIL's business.

Alternative emergency contacts

During the periods of recovery (as specified in this BCP) significant outages are largely addressed through the routing of incoming telephone calls and e-mails to the members of VIL's staff and temporary support employees located at VIL's parent investment company IC Veles Capital LLC (Moscow, Russia). Should the automatic routing be impossible all the interested persons are advised to use the following contact information of IC Veles Capital LLC with mentioning Veles International Limited at the start of each such communication:

Telephone: +7 495 258 1988
Fax: +7 (495) 258-1989
E-mail: mail@veles-capital.ru
Web-site: veles-capital.com

VIL's business continuity context

VIL is a Cyprus Financial Firm ('CIF') authorised by the Cyprus Securities and Exchange Commission (CySEC). As a CIF, VIL has a general duty to act honestly, fairly and professionally in its clients' best interests always striving to obtain, when executing their orders, the best possible result for the clients. As a general duty, VIL must safeguard its clients' assets and their personal data.

Essentially, client orders must be executed on a relevant (specified) financial market not later than on the day following the date of their receipt. Also, VIL has a duty to provide its clients with the necessary information as to its products and services before any service is rendered or a product is sold, as well as to provide the clients with the transaction reports not later than the business day following the day of the transaction (execution of the order). VIL is also obligated to respond to client complaints within five business days of their receipt.

As a regulated investment firm, VIL has a statutory duty to report transactions it performs to the CySEC on a daily basis, to submit various other reports less frequently and to respond to certain queries not later than on the following day after the receipt of such queries.

The seamless performance of duties listed in the two paragraphs above are considered *VIL's Minimum Business continuity objectives (MBCOs).*

Thus, the continuity of communications with the clients, authorities (primarily CySEC), market counterparties, stock exchanges, banks, custodians, brokers, market and financial data providers and other members of the financial markets infrastructure (*the Stakeholders*) are of major importance with the Internet connection and telephony being one of the main means of such communication. Equally important is the seamless functioning of the respective equipment (computers, servers, etc.) processing and storing client, market and regulatory data. Finally, as the majority of functions performed within VIL require high level of skills, qualification and knowledge of the specifics of VIL's business and its clientele, the ability to continually employ the respective members of staff and to ensure they operate safely and comfortably is always the utmost priority for VIL.

Given the MBCOs referred to in this section, *Maximum tolerable period of disruption ('MTPD')* is considered to be two days with the *Prioritized timeframes* and actions to be performed specified in the Annex 1 to this Policy.

Risk assessment and main continuity risks

VIL has taken the risk-based approach in designing its BCP adapting its plans to reflect its individual risk profile and the complexity of its activities. The types of business continuity threats and risks are subject to regular review: (1) on an annual basis, (2) when changes to the threat environment occur, or (3) when there is a substantive change in VIL's operations, e.g. an authorisation with respect to new activity has been obtained, new geographic areas have been entered into, scale of business has increased significantly, etc.

Threats and risks are identified in a full-threat-and-risk assessment with mitigating risks being an ongoing process.

Taking into account that i) the scale of VIL's business cannot be considered significant in terms of the number of its employees (less than 20), premises occupied (the single office in a well-maintained and equipped business center in Nicosia) and geographical presence (mainly Cyprus and Russia), on the one hand, and ii) the nature of its business itself is very sensitive to the skills of its staff and

reliability of hardware and software used, on the other hand, the main continuity risks can be summarized as follows.

- IT services risk - the risk posed to VIL's IT services, including communication channels, data-bases, operation software (trading, back-office, middle office, accounting, compliance and risk management applications) and hardware (computers, servers, network equipment and telephone stations), by natural disasters, riots, disruption of power supply, fire, equipment failure, cyber-crime, human error and fraud. IT services risk includes, for the purposes of this Policy, the risk posed to VIL's premises where the equipment is installed and the respective stuff normally operates;
- HR risk – the risk posed to VIL's staff (Human Resources) by natural disasters, catastrophes, incidents, epidemics and pandemic outbreaks, as well as other threats to human health, unexpected termination of employment and other situations where the access to critical human skills (including management and control skills) are temporary lost or limited.

Continuity risk mitigating measures

IT services risk

Mitigating measures directed at IT services risk are described in detail in Annex 1 to this Policy.

VIL outsources its IT function to the IT Department of its parent company IC Veles Capital LLC located in Moscow, Russian Federation which is closely involved in VIL's IT business continuity plan that deals with recovering IT services after a disastrous interruption.

Essentially, the appropriate level of IT services continuity is achieved with the following:

- IT Department of Veles Capital LLC provides information technology support and services to VIL and its employees. Services include IT planning and management, PC and server support, network and telephony support, software development and implementation, web development, database management etc.;
- there is a specific service desk, including the single point of contact between IT specialists and the employees. Tracking of users requests is carried out by the helpdesk software;
- various remote control tools, monitoring and notification systems are in place;
- IT support and administration are mainly carried out remotely, using:
    - 10 Mbs circuit between the offices
    - VPN-connection over the Internet duplicated the main circuit
    - telephone calls, remote control managers and other tools
- there are specific procedures in place to mitigate the risk of cyber-crime and data loss;
- IT documentation is always maintained up-to-date;
- business trips for work purposes are organized on a routine basis;
- third party support can be quickly applied for in case of extreme necessity;
- the time of recovery and particular recovery measures are provided for every type of disruption taking into account VIL's Minimum Business continuity objectives (MBCOs), Maximum tolerable period of disruption (MTPD) and the respective Prioritized timeframes as specified above in this Policy.

HR continuity risk

Essentially, the appropriate level of IT continuity is achieved with the following:

- every employee has an in-house alternate with adequate qualification and training. Particularly, the following list specifies the alternates (back-ups) of the management staff (executive directors and heads of departments):
    - CEO → 2-nd Four Eyes
    - Head of Brokerage → Any other Brokerage specialist approved by CEO
    - Head of Compliance → CEO
    - MLCO → Head of Compliance
    - Head of Middle Office → Head of Back Office
    - Head of Back Office → Any other Back officer approved by CEO
    - Head of Treasury → Any other Treasury officer approved by CEO
    - Head of Accounting → Any other Accounting officer approved by CEO
- VIL's parent company IC Veles Capital LLC has vast HR capabilities including employees and managers trained and certified in Cyprus and other EU states. These employees are familiar with VIL's and the group business and policies, can perform their functions at VIL remotely or can be relocated to Nicosia immediately in case of emergency. Importantly, due to the group rotation policy several core employees located in Moscow used to be employed by VIL having performed their jobs from the premises of VIL;
- Likewise, core employees of VIL can be immediately relocated to the premises of IC Veles Capital in case of the damages to the premises in Nicosia;
- VIL's internal audit function is outsourced to a highly reputed Cyprus company Delfi Corporate Services Limited which used to perform VIL's compliance function as well. Therefore, being familiar with the particularities of the business, this company is able to start performing any VIL's control function immediately according to the understanding agreed upon;
- two of the five VIL's directors are located in Moscow occupying director's positions within the group;
- there are training and competence process in place ensuring that junior employees achieve a sufficient level of professional competency. Uniquely skilled individuals are identified and cross-training and multi-tasking measures are provided for;
- all members of staff are subject to thorough vetting and testing before having been employed to minimize the risk of human error, negligence and crime;
- members of VIL's four eyes function, one of the three NED's and key staff are prevented from travelling together;
- medical insurance and vaccination is routinely provided by the group.

Other important measures

- all critical areas and systems of Veles Capital LLC supporting VIL's IT services and other relevant functions have their power supply backed up by the generators installed or in the process of being installed;
- if the water supply to the area where VIL's premises are located is discontinued or becomes contaminated, the site can remain open at least one week;
- there are 24/7 security service, internal and external CCTVs, access control systems and a standard procedure for receiving couriers and visitors;
- advanced fire detection and early warning systems are installed;
- evacuation tests are conducted at least annually under the supervision of the office provider.

Business continuity planning and governance

VIL's BoD and senior management understands the importance of thorough business continuity planning in order to be able to continuously deliver its services to the satisfaction of its clients. Business continuity planning is based on the continuity risk assessment conducted as provided for above in this Policy.

VIL's business continuity governance structure provides for a team that will ensure business continuity planning, senior management commitments and define senior management roles and responsibilities (the 'BC Planning team' or 'BCP team'). The BCP team comprises the CEO, one independent NED and the Compliance officer. The BCP team is responsible for the oversight, initiation, planning, approval, testing and auditing the BCP (with the support of the Internal Auditor). The composition of the Team ensures its members understand critical functions of VIL and are able to represent most of their continuity interests. It is the duty of the BCP team's coordinator (the CEO) to communicate business continuity policies and procedures clearly to VIL's staff.

Additionally, the Crisis management team with clearly defined duties and responsibilities (the 'CM team') is responsible for managing all critical internal and external issues of VIL to resolution of crisis situations. The CM team comprises VIL's four eyes with the support of the Compliance officer. The CM team is responsible for designing and implementing a crisis management communication plan which covers internal and external communications with staff, clients, regulators, counterparties, the media and other stakeholders. The plan includes Alternative emergency contacts, specified in this Policy, which are used for communicating with VIL from the outside. It will also contain internal instructions, means of communication and status information to be provided to staff at the start of a crisis situation and during the crisis.

VIL's BoD reviews and approves all updates and changes in the BCP, which appear on the BoD's agenda at least bi-annually. VIL's business continuity planning and the effectiveness of relevant policies, procedures, systems and controls are subject to annual Internal Audit review and assessment and are included in a clear, documented and approved audit cycle covering all departments and functions.

Business continuity awareness and training

To ensure staff is aware of VIL's business continuity policies and procedures:

- business continuity is included in induction programs for new employees;
- all staff are made aware of the BCP and of the roles, responsibilities and organisation of the BC planning team and Crisis Management team;
- senior management and all staff are familiar with their role during a major operational disruption;
- the staff job descriptions should clearly state which members of staff are required at the alternate facility and which can go home;
- all staff have been trained and have been involved in business continuity tests;
- HR strategy supports business continuity;
- all departments' heads know their planned (minimum) staffing levels in an incident.