Information policy, information technology and information security governance

The Board is responsible for information governance within UBP and the management of information technology and information security governance are delegated to the IT function. In this respect, the existing policies are detailed hereunder:

Acceptable use policy

The purpose of this policy is to ensure that employees, contractors and third parties are aware of the appropriate and acceptable use of assets.

E-mail acceptable use policy

The policy aims to outline appropriate and inappropriate use of e-mail systems and services in order to minimize disruptions to services and activities, as well as to comply with applicable policies and laws. This policy includes the company's email system in its entirety.

Internet acceptable use policy

The objective of this policy is to outline appropriate and inappropriate use of internet resources, including the World Wide Web, electronic mail, the intranet, FTP (file transfer protocol) and USENET.

System administrator policy

The purpose of this policy is to establish the expectations for employees who have administrative and privileged access rights to the Company's IT systems and confidential information.

Remote access policy

The purpose of this policy is to define standards for connecting to UBP Group's networks from any host outside of the Group's boundaries. The standard detailed below are designed to reduce the potential risk and exposure to UBP from damages which may result from unauthorized use of UBP Group resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical UBP internal systems, and fines or other financial liabilities incurred as a result of those losses.

Teleworking policy

The purpose of this policy is to ensure that security of information and systems, accessed through teleworking is given due importance. It is essential that employees understand and adhere to existing security procedures and policies. Information that is related to and can identify an individual is personal data and protected by the principles of the Data Protection Regulations. As such, appropriate technical and organisational measure shall be taken against accidental or deliberate loss, change, destruction of, or damage to personal data. These

procedures have been produced to ensure that protection of personal and corporate data are maintained whilst remote working.

Logical Access policy

The objective of this policy is to limit access to information, information processing facilities and business processes within UBP Group.

Malicious and Mobile Code Policy

The objective of this policy is to protect the integrity of software and information from malicious attacker gaining access to network, virus or other malware infecting computers. The purpose of this policy is to provide instructions on measures that must be taken by employees to help achieve effective malware detection and prevention. This policy covers any mobile device capable of coming into contact with your companies' data.

Information security Policy

The objective of this policy is:

-To ensure the business continuity of -UBP by protecting its information assets from all threats, whether internal or external, deliberate, environmental or accidental:

-To minimise the risk of damage by preventing security incidents and reducing their potential impact.

Media handling policy

The objective of this policy is to ensure that media are controlled and physically protected, to prevent unauthorized disclosure, modification, removal or destruction of information stored on media and consequent interruption activities.

Back-up policy

The objective of this policy is to protect against loss data, maintain the integrity and availability of information and information-processing facilities by taking and testing regularly backup copies of information and software.

Network security policy

The objective of this policy is to ensure the protection of information in specific networks and the protection of the supporting infrastructure This policy might include specific procedures around device passwords, logs, firewalls, networked hardware and/or security testing.

Password policy

The objective of this policy is to safeguard the company from cyberattack. It sets a standard for creating, protecting and changing passwords in order to ensure that they are strong, secure and protected and to compromise the company's entire corporate network.

Information Security Incident Management Policy

The objective of this policy is to ensure that information security events and weakness associated with information systems are communicated in a manner allowing timely corrective action to be taken. It also ensures that a consistent and effective approach is applied to the management of information security incident. This policy covers all incidents that may affect the security and integrity of UBP's information assets and outlines steps to take in the event such an incident occurs.

Compliance Policy

The objective of the compliance policy is to avoid breaches of any laws, statutory, regulatory or contractual obligations and of any security requirements. It is also to ensure compliance of systems with organisational security policies and standards.

Laptop Policy

The purpose of this policy is to provide guidance in order to minimize information security risks that may affect laptops.

BYOD Policy

The purpose of this policy is to set out the controls that must be in place when using mobile devices that are not owned or provided by the organisation but used for the business purposes.

IT Business Continuity Policy

The objective of this policy is to ensure that an IT Business Continuity Plan is developed, documented, continuity tested, reviewed and updated in order to enable the UBP Group to recover as quickly and effectively as possible from any unforeseen disaster or emergency with minimised business interruptions and ensure proper communication internally and externally.