Information Security Policy

Document title	Information Security Policy		
Reference No.	InfoSec	**Version**	1.1
Author	Saul Muscat, Head of Enrolments (DPO)		
Reviewed by	Pete Faulkner, IT Manager		
Authorised by	Luke Muscat, Group CEO		
Issue date	23/03/2023		
Review due	24/06/2025		

DOCUMENT CONTROL

Version	Name	Comment	Date
1.0	A Dann	New Issue	01/02/2020
1.0	S Muscat	Review	18/09/2021
1.0	P Faulkner	Review	21/02/2022
1.1	S Muscat	Review + minor amendments	23/03/2023
1.1	S Muscat	Annual Review	24/06/2024

Information Security Policy

Introduction

1 The B2W Group has an ethical, legal and professional duty to ensure the information it holds conforms to the principles of confidentiality, integrity and availability. In other words, the information B2W is responsible for is safeguarded where necessary against inappropriate disclosure, is accurate, timely and attributable, and is available to those who should be able to access it.

2 This information security policy outlines B2W's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the Group's information systems.

3 Under that umbrella, supporting policies, procedures and guidelines provide further detail on how to implement those information security arrangements.

Objective

4 The main purpose of this policy is to describe the minimum level of protection that B2W expects of all B2W's information systems to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.

5 A secondary but very relevant purpose of this policy is to ensure that all users understand their responsibilities for protecting the confidentiality and integrity of the data that they handle, including making users aware of relevant legislation.

6 The directives set in this policy are defined with the overarching objectives:

a. To support the B2W business objectives in a flexible and effective way
b. To maintain adequate regulatory compliance
c. To protect B2W's information assets
d. To maintain business continuity

7 The policy of B2W is to protect information systems from unauthorised access, use, disclosure, destruction, modification, disruption or distribution.

8 The B2W Senior Management Team will ensure business, legal, regulatory requirements and contractual information security obligations are met.

9 This policy is the cornerstone of B2W's on-going commitment to establish and maintain our information security procedures.

Scope

10 This policy is applicable to all staff, students, other members of B2W and third parties who interact with information held by B2W and the information systems used to store and process it. This includes, but is not limited to, any systems or data attached to B2W data or telephone networks, systems managed by B2W, mobile and personal devices used to connect to B2W networks or hold B2W data, data over which B2W holds the intellectual property rights, data over which B2W is the data owner or data custodian, communications sent to or from B2W.

Roles and responsibilities

Responsibilities of every user of B2W IT resources, including Third Party Service Providers

11 Staff, Students and -in general- users of B2W IT resources are expected to meet the acceptable usage policies and related terms and conditions of the services provided by B2W and by any third party on our behalf (e.g. Microsoft software licensing agreements).

12 B2W will provide tools to create and store data, connect to the Internet and other networks. Users must apply these in a legal and appropriate manner, to protect the personal safety of themselves and their peers and to ask B2W staff for advice or assistance in case of doubt or concerns. The IT Team should be the first point of contact.

13 Users must manage passwords with care and processes should be in place to ensure confidentiality from the initial creation, storage in applications, communication and day to day usage.

Responsibilities specific to every B2W Group Staff Member

14 All employees and third parties using B2W systems are accountable for understanding and following B2W's information security policies, as well as promoting safe practices within their teams and monitor compliance.

15 All employees and third parties are responsible for asking for assistance when in doubt about how to proceed or interpret a policy and also to report any concern or suspect activity encountered. Depending on the nature of the concern, the first point of contact should be one of these: the line manager, IT Team or Human Resources.

Responsibilities specific to Managers

16 Fully understand the data, people, systems and processes that he/she is accountable for its safeguard

a. B2W managers are expected to identify the data and systems under their remit and accept accountability for its protection. Individual "custodians" (also referred as "owners") of the data will be identified. They will be accountable for it and will make informed decisions on risks and appropriate levels of protection, on behalf of B2W.

17 Strategic support to open networks

a. B2W managers should not exclusively rely on perimeter controls, but also implement (or fund) security on each individual system. In an open and dynamic organisation such as B2W, having a clear strategy of providing flexible and seamless mobile access, it is no longer effective to rely on broad "Internet vs internal" networks, or physical access to the offices or on user ignorance of our estate or IT tools, to protect B2W from accidental or intentional misuse.

18 Back secure systems

a. B2W managers that sponsor a system to process B2W data are accountable for commissioning one that meets the information security policy, applying deliberate and verifiable risk management. Security measures need to be identified, designed, resourced and delivered from the start of any initiative alongside any other business functionality and maintained for the entire lifecycle of the process or IT system, up to the data and system disposal.

19 Support services to deliver their services securely and be custodian/gatekeepers of the systems

a. Central functions such as the IT Team, Human Resources and Finance will support the delivery of security on an "internal service provider" model. These functions will also have the mandate to monitor compliance and where appropriate will have accountability for the custodianship/gatekeeping in maintaining the practices agreed/accepted by the Board of Directors.

20 Setup resilient business processes, with a combination of controls to avoid single points of failure
   a. B2W managers should ensure that the risks of concentrating functions on a single control ("single point of failure") - whether performed by individuals or systems- are well understood and actively managed. Managers need to choose and implement the combination of preventative and monitoring controls that best meet the business objectives.
21 Ensure their teams are security savvy
   a. B2W managers should ensure their teams have the necessary skills and should communicate their responsibilities regarding protecting systems and data.
22 Oversee their teams and systems are effective
   a. B2W managers should actively, regularly and demonstrably verify what their reports are doing and how systems under his/her supervision are functioning (with the assistance of the IT Team where appropriate).
23 Monitor the third party with access to B2W systems and data
   a. B2W managers should ensure any subcontractor employed for a particular function will meet the requirements specified (on selection and on an ongoing basis) and accept responsibility for their actions.

Responsibilities of Senior Management

24 Risk Ownership
   a. The Board of Directors owns the overall risk management process, and the prioritisation and acceptance of risks. Risks are identified "bottom up" from each department and "top down" from the Board of Directors in a two-way flow.
25 Risk Acceptance
   a. Managers, individually or via governing bodies have the accountability for taking a stance on risks within their authority (or escalating if exceeds it) and ensuring the business operates in line with the Board of Governor's expectations.
26 Risk Treatment
   a. In conjunction with the MIS and Compliance Manager, the Contracts Manager and the IT Team and the Board of Governors will help identify risks to B2W. The Board of Directors will take advice from these and other sources. Ultimately the responsibility for risk lies with the Board of Directors.

Responsibilities of the MIS and Compliance Manager, the Contracts Manager and the IT Team

27 Risk management
   a. Identify threats to B2W's information assets and advise on impact and recommended remediation. Scope includes risks related to information, data, technology & related regulatory requirements.
28 Policies and education
   a. Communicate acceptable levels of risk and mitigation practices throughout B2W via policy, standards and awareness programs.
29 Measuring progress and compliance
   a. The information security programme will perform validation of compliance directly on the processes or verifying the management controls.
30 Incident response
   a. Develop central capabilities to effectively respond to significant information security related incidents.
31 Service delivery
   a. There may be central services delivered by the IT Team, for example on demand pen testing, or some diagnostics/checks.

Responsibilities specific to Third Party Providers

32 Meeting terms of service/contract agreements, right to audit.
   a. Third party shall adhere to the IT acceptable usage policy as well as any other requirements specified in the service contract.

33 Security and incident response tests.
   a. Third party working for B2W are expected to participate in incident response tests or drills as any other member of staff, when using B2W resources and/or premises. Specific audit/reviews/checks might be undertaken on external service providers, due to the dynamic nature of such relationships.

Policy Management, Education and Awareness

34 Policies as minimum expectation for risk management
   a. Managing risks is an essential part of the business activity at all levels of the organisation. The information security policies are only the minimum expectation to address information security risks according to well established practice. Management should assess the business, legal, contractual and corporate social responsibility risks and requirements in each relevant jurisdiction to decide on the need for additional controls or exceptions, and be able to justify and be accountable for these decisions..

35 Policy issuing, communication and updating
   a. A set of policies and procedures for information security will be maintained, approved by management, published and communicated to employees and relevant external parties. These policies should follow the overarching framework for policy approval and review defined at B2W level. In particular, policies should be reviewed and updated at least annually.

36 Trust, but verify
   a. The policy statements are necessary but not sufficient on its own. There needs to be controls in place to provide comfort that policies are being followed. Furthermore, those controls should not be transactional or preventative only; Managers should perform demonstrable "controls over the controls" at an appropriate level of detail to reasonably conclude they are effective.

37 Awareness and education on policies and procedures
   a. Managers should ensure staff and external parties working with B2W systems and data are formally aware of and educated on the policies and procedures they must be compliant with. This is a fundamental step to establishing any individual's accountability.
   b. All new employees must undertake mandatory training on Information Security prior to having access to personal or sensitive data.
   c. Existing employees must undertake mandatory training on Information Security on an annual basis,

Human Resource Activity

38 Acceptable use of B2W resources
   a. Every employee and third party granted access to B2W systems and/or data has a responsibility to use the systems and data in a secure manner, for B2W business purposes, following B2W policies and applying good judgment. Only approved hardware, software and data should be used to perform B2W business.

39 Responsibility for reporting non-compliance
   a. Users are responsible for reporting:
      - any concern on how the security processes are performing;
      - any suspected or confirmed incident regarding unauthorized or incorrect use to their manager, the IT Team, Human Resources or a Senior Manager.

40 Management responsibility for security
   a. Management is responsible for requiring their teams of employees and contractors to apply information security according to established policies and procedures, and to monitor use within his/her teams, leading by example and ensuring their direct reports have been educated on policies and security practices.
41 Background checks on employees
   a. Background verification checks on candidates for employment, employees or contractors, as established by Human Resources, shall consider explicitly the sensitivity of the information to be accessed and the perceived risks when defining the nature and timing of those checks.
42 Terms and condition of employment and termination or change of responsibilities
   a. The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security including those that remain after termination or change of functions. Detail procedures should be documented and communicated to the employee or contractor and enforced.
43 Enforcement of information security policies
   a. The HR department is responsible for defining and communicating the disciplinary process applicable to employees who have committed an information security breach.

Data/Assets Management

44 Data classification
   a. Each department manager must identify the data being used for fulfilling their duties and adopt controls to protect the information according to its risk. Assigning ownership and a sensitivity classification is a highly recommended method of protecting assets efficiently. If no formal classification is used, the department should work on the assumption that all information is as critical as the most critical information they possess.
45 Retention of information
   a. B2W will have processes in place to safely dispose of information as required by law or, within legal compliance, when is no longer cost effective to retain. Based on their remit, Managers, assisted by legal counsel, is responsible for defining the acceptable retention period for the various kinds of data they hold. Managers are also responsible for establishing the controls to ensure these criteria are followed.
46 Safe storage and disposal of electronic media and surplus hardware
   a. The IT Team will define a formal procedures in place for the safe acceptance, storage and disposal of surplus technology hardware (including electronic storage media). B2W only accepts new, vendor guaranteed equipment and destroys surplus/failed equipment/media/paper securely, compliant with the law, and (then) in an environmentally friendly way. Other arrangements need to be dealt on a case by case with business and technical signoff.
47 Safe storage and disposal of paper
   a. The MIS and Compliance Manager, the Director responsible for HR and the Finance Director will define relevant formal procedures for the safe storage, retrieval and disposal of paper files.
48 Logs retention policy
   a. As a general rule, any logging activity should be kept for at least one year, of which three (3) months should be online immediately accessible upon request from a governing body or external inspection. Management needs to familiarise with local contractual/legal requirements applicable to each business to determine if additional requirements apply, or a shorter retention is acceptable.

49 Physical security, controlled areas
   a. B2W assets, including systems and media need to be protected against intentional or accidental physical damage. For that, they will be located in an area with restricted access and protected against environmental hazards, under full control of B2W.

Security by Design, Secure Architecture, Acquisition and Development

50 Protection from malware
   a. The default approach is that all B2W systems should have detection, prevention and recovery controls to protect against malware combined with appropriate user awareness. Exceptions need to be formally approved on a case by case basis by Senior Management.
   b. Software should be configured to scan files automatically upon access and when they area accessed by a network folder
   c. Software should scan web pages automatically when they are accessed through a web browser
   d. Software should prevent connections to malicious websites

51 Minimum security features in systems
   a. Systems should be developed/acquired and configured with the security features necessary to enable enforcement of the following:
      i. Users can only access data and functionality for which they are authorised ("least privileges" approach)
      ii. Accountability for usage is maintained via appropriate audit trails where available.
      iii. Availability and integrity of the systems, including disaster recovery (DR) arrangements are addressed. These should be included in services agreements.

52 Secure development and Vulnerability Management in the IT infrastructure
   a. All systems must be developed/configured following practices that specifically identify and minimise vulnerabilities, and subsequently, processes will be in place to promptly address newly discovered vulnerabilities according to their criticality.

53 Installation of software, patching
   a. Software installation should be restricted to users approved by the IT Team. Only licensed software, approved by the IT Team is allowed to be installed on systems. Installation of software updates should be managed by the IT Team.Device verification.

54 Device verification
   a. Any devices used to access commercially sensitive or personal data should be blocked unless they are connected to Microsoft Intune
   b. The IT team should ensure that all protection policies are kept up to date within in Intune Intune

55 Installation and Management of Firewalls
   a. Firewalls must be installed on B2W networks
   b. Remote administrative access should be disabled any access should be controlled by a 2 step authentication process.
   c. All inbound connections to be blocked as a default setting with any exceptions to be documented and agreed by the Managing Director
   d. Permissive firewall rules should be disabled as soon as they are no longer needed
   e. Host based firewalls are to be used on any devices that may be used on untrusted networks such as public wi-fi.

Technical and Operational Security

56 Protecting the business processes stability
   a. The IT Team and the Business Management that owns the system have a joint responsibility for defining operational procedures and training users to ensure the secure operations of the processing facilities.
   b. Changes and tests on live (i.e. Production) systems including servers and end-user devices should be conducted in a controlled manner. Direct changes in production, un-announced tests/hacking, or intentionally creating a failure are not authorised by default.

57 Monitoring and duty of care
   a. The IT Team has a mandate to monitor the performance, integrity and overall confidentiality of the systems and have the technical knowledge and authority to apply measures to protect the overall infrastructure against threats, following normal or emergency procedures.
   b. B2W reserves the right to monitor individual's usage, to the extent granted by the law, in order to protect its legitimate business interests. Monitoring may include accessing stored or transmitted data as well as observation of user activity.
   c. B2W has also a "duty of care" obligation to reasonably monitor usage of company resources to detect abuse in breach of the law, and to report to the appropriate authorities.

58 Logging and Auditing policy
   a. By default system logs should be enabled to capture user logon, exceptions, faults and information security events/alerts.

59 Change management and security
   a. B2W has a policy of using 3rd party hosting and software provision, and thus as part of the software agreements with these 3rd parties, it is their responsibility to provide updates to software in a managed manner.

60 Physical and environmental security
   a. Equipment shall be installed with appropriate protection from environmental factors and unauthorised access, in line with the sensitivity of the data and business process it supports. All equipment by default should be provisioned, installed and managed by the IT Team, with vendor warranty and maintenance in place. Exceptions include vendor managed installation and pre-approved decentralised purchases.

61 Data backup and restore procedures
   a. Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup plan approved by the data/system owner/vendor managed systems agreement. As a default/minimum criteria, backups plans should allow restore at any point of past 30 days, plus last 12 months of monthly snapshots stored in a different location than the system being backed up. Backups should be stored encrypted, under physical security and inventory control. Restore tests of the media/files should be done at least once a year.

62 Vulnerability Scanning
   a. All systems should be subject to regular vulnerability scans (at least every 12 months and after any significant change has been made to a system). These scans may be undertaken by appropriately skilled internal staff or by approved external assessors. Business critical systems

and other systems which are used to process or store data classified as strictly confidential or above should be subject to regular (at least annual) penetration testing by an approved external assessor.

Access Management

63 Due diligence before granting access
   a. Access to systems and information, including setting up permanent network connectivity solutions, will be granted to employees and third parties/service providers only after a due diligence risk assessment has been performed and after the employment or service contracts, including confidentiality and accountability clauses has been agreed in writing. Processes should be in place to ensure ongoing monitoring of compliance.

64 Business management responsibility for access control
   a. Each Business Unit must have a consistent process to approve modify and remove, as well as regularly review the access granted to users on systems and information he/she is accountable for, and monitor the usage of the system, with assistance and tools provided by the IT Team.
   b. User accounts should be removed or disabled as soon as they are no longer required

65 Minimum standard for authentication
   a. All enabled accounts in computer systems must have passwords or a comparable authentication method to establish user accountability. If using passwords, these need to have system enforced complexity, expiration, reuse and lockout controls. System enforced session timeout is desirable. Passwords and other secret information needed for authentication should not be transmitted over the networks or stored in the clear (i.e. needs to be encrypted).
   b. Users must be authenticated before having internet-based access to commercially sensitive or personal data.
   c. Any auto-run feature that allows file execution without user authorisation and authetication should be disabled.

66 Individual accountability
   a. Systems and procedures should ensure activity in the systems or with IT assets can be linked to an individual. When the individual is not an employee, the manager accountable for allowing and monitoring such access should be clearly identified. If the account is used by another system, there still need to be an appointed individual responsible for the setup and system credentials and generally the safeguarding of that account.

67 User accountability for security
   a. All employees and third parties using B2W's systems are accountable for understanding and following B2W's security policies, in particular on how to protect their accounts and passwords from misuse. All employees are expected to report any concern or potential suspect activity they may encounter. Employees should contact their line manager, the IT Team, Human Resources or Senior Management for clarification or assistance.

68 Privileged access to systems
   a. All privileged/administrator activity (e.g., ID and password creation, direct access to data, maintenance, and support) must be traceable to the individuals whether directly accountable for these activities, or indirectly accountable, in the case of automated processes.

Incident Management

69 Incident Management Policy

a. Guidance will be available on what constitutes an Information Security incident and how this should be reported. Actual or suspected breaches of information security must be reported and will be investigated. Appropriate corrective action will be taken and any learning built in to controls.

70 Contact with authorities

a. Appropriate contacts with relevant authorities and external entities (e.g. the Press) shall be maintained. In case of an incident, only nominated contacts are authorised to liaise with authorities and external entities, as instructed by the Board of Directors.

71 Responsibilities of staff and students

a. If a member of B2W (staff or student) is aware of an information security incident, then they must report it to the Data Protection Officer. If necessary, members of B2W can also use the institutional whistle blowing process.

Business Continuity and Information Governance

72 Business continuity is governed by the Business Continuity Policy

a. This section deals with the information governance concerns to support continuity planning.

73 Business critical electronic systems for processing and storing information

a. Systems should preferably be SaaS based to allow password protected remote access in the event of a disaster or major incident
b. Data should be held on b2w's cloud based storage areas to allow remote access and recovery in the event of an incident
c. All Office 365 accounts to include we based access with information and data stored for 90 days as a default setting.
d. Where systems are reliant on B2W networks it is the responsibility of the IT Team to ensure that systems can be accessed in the event of a disaster or network failure
e. All systems for processing and storing data should be routinely backed up to a cloud based server.
f. All systems must be routinely tested to ensure that electronic protocols supporting continuity are effective.

74 Paper based systems for collection and storage

a. Where paper based systems are used for the collection of storage , it is the responsibility of the relevant departmental managers to ensure that electronic alternative methods are available should they be required. For example, electronic enrolment forms.
b. Storage of paper-based records should include considerations for disasters such as fire and flooding with safeguards in place to ensure the security of records in such events.
c. Where paper based records are critical to business operations they should be converted to electronic formats and stored on cloud based storage areas.

Compliance, Validation and Certification Initiatives

75 Compliance with the law

a. B2W and each employee is accountable for operating within the law, and it is their responsibility to be aware of legal and contractual requirements and implement the controls within their remits to comply.

76 Information security in contracts with third party

a. Service Providers with access to B2W systems and data must contractually commit to implement security measures to meet the business objectives (e.g. protecting intellectual property, availability) as well as regulatory or contractual obligations for which B2W has ultimate accountability.

77 Supplier service delivery management

a. The manager that owns the service is responsible for regularly monitoring, review and audit supplier service delivery. Information Security considerations, including protecting B2W intellectual property and maintenance of regulatory compliance requirements should be explicit in this review.

78 Management controls

a. Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. Evidence of the performance of such controls should also be kept.

79 Internal and independent security reviews

a. The information security programme and its implementation shall be reviewed at planned intervals or when significant changes occur. It is expected that evidence of the controls performed by employees/systems as well as any controls management performs over them (also called "second tier" or "control over the control") are kept.

Glossary

Access Control - ensures that resources are only granted to those users who are entitled to them.

Appropriate - suitable for the level of risk identified and justifiable by risk assessment.

Asset – anything that has a value to B2W

Audit - information gathering and analysis of assets, processes and controls to ensure policy compliance.

Authentication - is the process of verifying a claim of identity. Three different types of information can be used for authentication: something you know (a PIN, a password, mother's maiden name), something you have (magnetic swipe card) or something you are (biometrics).

Availability – information and supporting IT systems should be available to authorised users when needed.

Confidentiality - information is disclosed only to those who are authorised to view it.

Control – a means of mitigating risks by providing safeguards. This includes policies, procedures, guidelines, other administrative controls, technical controls or management controls.

Data - Information held in electronic or hard copy form.

Information - Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual.

Information Asset Owner – is a person or entity that has been given formal responsibility for the security of an information asset.

Information Security – preservation of confidentiality, integrity and availability for information and supporting IT systems.

Information Systems – any system, service or infrastructure used to process information or the physical locations housing them. This includes critical business environments, business processes, business applications (including those under development), computer systems and networks.

ISO/IEC 27001:2013 - information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), entitled Information Technology – Security Techniques – Information Security Management Systems – Requirements.

ISO/IEC 27002:2013 - information security standard (list of controls) published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), entitled Information Technology – Security Techniques – Code of practice for Information Security - Controls.

Integrity - maintaining and assuring the accuracy and consistency of information over its entire life-cycle. It should not be possible for information to be modified in an unauthorized or n undetected manner.

Policy – overall intention and direction as formally expressed by management.

Risk - the potential for an unwanted event to have a negative impact as a result of exploiting a weakness. It can be seen as a function of the value of the asset, threats and vulnerabilities

Risk Assessment – overall process of identifying and evaluating risk.

Third party – person or body that is recognised as being independent of B2W.

Threat – something that has the potential to exploit a weakness to result in some form of damage. Threats can be environmental, deliberate, accidental, logical or technical.

Vulnerability – weakness of an asset or group of assets that may be exploited by a threat.

Questions about this policy should be referred to both:

HR@b2wgroup.com and IT@b2wgroup.com