INFORMATION SECURITY POLICY

Burjeel Holdings PLC

1. Introduction

The confidentiality, integrity and availability of information are critical to the functioning and good governance of Burjeel Holdings PLC including its affiliates and subsidiaries ("Burjeel"). Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for Burjeel to recover. This information security policy (the "Policy") outlines Burjeel's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of Burjeel's information systems. Supporting policies, codes of practice, procedures and guidelines provide further details. Burjeel is committed to a robust implementation of information security management. It aims to ensure the appropriate confidentiality, integrity and availability of its systems and data, including proactive measures to ensure our IT environment is built, maintained and governed in the right ways. The principles defined in this Policy will be applied to all electronic information assets for which Burjeel is responsible. Burjeel is specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of third parties pursuant to the carrying out of work agreed by contract.

1.1 Objectives

The objectives of this Policy are to:

1. Provide an information security framework covering all Burjeel information systems (including but not limited to all cloud environments commissioned or run by Burjeel, computers, storage, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems. It requires that:

a. The resources required to manage such systems will be made available.

b. Continuous improvement of Burjeel's information security management system will be undertaken.

2. Make certain that users are aware of and comply with all current and relevant UAE laws.

3. Provide the principles by which a safe and secure information systems environment can be established for employees and any other authorised users.

4. Ensure that all users understand their responsibilities for protecting the confidentiality and integrity of the data that they handle.

5. Protect Burjeel from liability or damage through the misuse of its IT facilities.

6. Maintain healthcare data and other confidential information at a level of security commensurate with its classification including upholding legal and contractual requirements around information security.

7. Respond to changes in the context of the organisation as appropriate, initiating a cycle of continuous improvement.

1.2 Scope

This Policy is applicable to all employees of Burjeel and its affiliates and subsidiaries and all directors, officers, employees, permitted assigns, and other third parties acting on behalf of the foregoing who interact with information held by Burjeel and the information systems used to store and process it. This includes, but is not limited to:

- Cloud systems developed or commissioned by Burjeel,
- systems or data attached to Burjeel networks,
- systems managed by Burjeel,
- mobile devices used to connect to Burjeel networks or hold Burjeel data,
- data over which Burjeel holds the intellectual property rights,
- data over which Burjeel is the data controller or data processor (wherever held),

2. Policy

2.1 Information security principles

The following information security principles provide overarching governance for the security and management of information at Burjeel.

1. Information should be classified according to an appropriate level of confidentiality, integrity and availability (see Section 2.3. Information Classification) and in accordance with relevant legislative, regulatory and contractual requirements.

2. Users with responsibilities for information (see Section 3. Responsibilities) must:

a. ensure the classification of that information is established;

b. handle that information in accordance with its classification level;

c. abide by Burjeel policies, procedures, and any contractual requirements.

3. All users covered by the scope of this Policy (see Section 1.2. Scope) must handle information appropriately and in accordance with its classification level.

4. Information should be both secure and available to those with a legitimate need for access in accordance with its classification level. Access to information will be on the basis of least privilege and need to know.

5. Information will be protected against unauthorized access and processing.

6. Breaches of this Policy must be reported (see Section 2.7. Incident Handling).

7. Information security systems will be regularly checked with penetration testing.

8. Explicit information security management systems (ISMSs) run within Burjeel will be appraised and adjusted through the principles of continuous improvement.

2.2 Legal & Regulatory Obligations

Burjeel has a responsibility to abide by and adhere to all current UAE legislations as well as regulatory and contractual requirements.

2.3 Information Classification

1. Below are the information classification levels that have been adopted by Burjeel and which underpin Burjeel's principles of information security.

2. These classification levels explicitly incorporate the legislative definition of personal data and special categories of personal data, as laid out in Burjeel's Data Protection Policy, and are designed to cover both primary and secondary research data.

3. Information may change classification levels over its lifetime, or due to its volume.

1. Confidential: Normally accessible only to specified members of Burjeel employees. Should be held in an encrypted state outside Burjeel systems; may have encryption at rest requirements from providers.

2. Restricted: Normally accessible only to specified and / or relevant members of Burjeel employees.

3. Public: Accessible to all members of the public.

2.4 Third Parties

All third parties doing business with Burjeel will abide by Burjeel's Information Security Policy, or otherwise be able to demonstrate corporate security policies providing equivalent assurance. This includes:

a. when accessing or processing Burjeel assets, whether on site or remotely.
b. when subcontracting to other providers.

2.5 Cloud Providers

Under the applicable laws, a breach of personal data can lead to heavy fines. Where Burjeel uses cloud services, it retains responsibility as the data controller for any data it puts into the service, and can be fined for a data breach, even if this is the fault of the cloud service provider. Burjeel also bears responsibility for contacting the data subject and regulatory authorities concerning any breach of its data, as well as any affected individual or patient. Burjeel must therefore be able to judge the appropriateness of a cloud service provider's information security provision. This leads to the following stipulations:

1. All providers of cloud services to Burjeel must respond to Burjeel's cloud assurance assessment prior to a service being commissioned, in order for Burjeel to understand the provider's information security provision. This is without prejudice to data privacy notifications.

2. Cloud services used to process personal data will be expected to have ISO27001 certification or equivalent controls, with adherence to the standard considered the best way of a supplier proving that it has met the applicable legal principle of privacy by design, and that it has considered information security throughout its service model.

3. Any request for exceptions, where the standards of security cannot be demonstrated to meet ISO27001 will be considered by the Compliance Officer and the General Counsel.

2.6 Compliance, Policy Awareness and Disciplinary Procedures

1. Compliance with this Policy is mandatory.

2. Mandatory user awareness training will accompany this Policy.

3. All current employees and other authorised users will be informed of the existence of this Policy and the availability of supporting policies, codes of practice and guidelines.

4. Any security breach will be handled in accordance with all relevant policies and the appropriate disciplinary policies.

2.7 Incident Handling

1. If an employee of Burjeel is aware of an information security incident then they must report it to the *itassist@burjeelholdings.com*

2. Breaches of personal data must be reported to the data subject (i.e. owner of the personal data) and the Compliance Officer.

3. All employees of Burjeel must report instances of actual or suspected phishing to *itassist@burjeelholdings.com*

2.8 Supporting Policies, Codes of Practice, Procedures and Guidelines

1. Supporting policies have been developed to strengthen and reinforce this Policy statement. These, along with associated codes of practice, procedures and guidelines will be published together and available on Burjeel's website.

2. All employees and any third parties authorised to access Burjeel's network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

3. Responsibilities

A. Employees of Burjeel:

All Employees of Burjeel, agency employees working for Burjeel, third parties and collaborators on Burjeel projects will be users of Burjeel information. This carries with it the responsibility to abide by this Policy, supporting policies and relevant legislation. No individual should be able to access information to which they do not have a legitimate access right. Notwithstanding systems in place to prevent this, no individual should knowingly contravene this Policy, nor allow others to do so. To report data breaches, please see Section 2.7: Incident Handling.

B. Information Technology Team:

Responsible for:

1. the information systems both manual and electronic that support Burjeel's work. This includes ensuring that data is appropriately stored, that the risks to data are appropriately understood and either mitigated or explicitly accepted, that the correct access rights have been put in place, with data only accessible to the right people, and ensuring there are appropriate backup, retention, disaster recovery and disposal mechanisms in place.

2. the security of information produced, provided or held in the course of carrying out research, consultancy or knowledge transfer activities. This includes ensuring that data is appropriately stored, that the risks to data are appropriately understood and mitigated, that the correct access rights have been put in place, with data only accessible to the right people, and ensuring there are appropriate backup, retention, disaster recovery and disposal mechanisms.

3. ensuring that the provision of Burjeel's IT infrastructure, cloud environments and applications is consistent with the demands of this Policy and current good practice.

4. ensuring third parties doing business with Burjeel has the proper level of security, as appropriate.

5. responding to cyber security issues, incidents or weaknesses.

6. reporting any incidents or weaknesses to the Compliance Officer and the General Counsel.

C. Compliance Officer:

Responsible for reporting any incidents or weaknesses to the competent regulatory authorities in accordance with applicable laws.

4. Policy Approval

This Policy shall be reviewed and approved by the Company's Board. This Policy shall be effective from the date of approval by the Board. All amendments to this Policy will be done in compliance with applicable laws and will require approval by the Board. The Chief Information Security Officer is the custodian of this Policy.

5. Documentation and Regular Review

Organization Scope	Burjeel
Parent Process	Compliance Program
Document owner	Chief Information Technology Officer
Approved by	Burjeel Board of Directors
Initial date published	February 10, 2023

Document effective date	February 10, 2023
Document updated as per	-
Contact person	Chief Information Technology Officer
Version	1.0

Burjeel’s Chief Information Security Officer shall periodically evaluate the effectiveness of this Policy, and review and revise it as necessary, including to reflect any changes required by applicable laws. You can direct any suggestions for improvements to this Policy to Burjeel’s Chief Information Security Officer at irshad@burjeelholdings.com.