docree.

Information Security Policy (Staff)

COMPANY	Docree Demo Broker Ltd
REGISTRATION	HE 000000
LICENSE	SAMPLE/00/0000
EFFECTIVE DATE	November 28, 2026
VERSION	v1.0

Table of Contents

01 Scope

02 Account Security

03 Acceptable Use

04 Data Handling

05 Device and Remote Work

06 Incident Reporting

07 Consequences

SECTION 01

Scope

1.1 This Information Security Policy (the "Policy") applies to all employees, contractors, and third parties who access Docree Demo Broker Ltd's (the "Company") information systems, data, or networks.

1.2 Compliance with this Policy is mandatory. Personnel are expected to protect the Company's information assets as a condition of their employment or engagement.

SECTION 02

Account Security

2.1 All personnel shall:

- Use strong, unique passwords of at least 12 characters, combining letters, numbers, and symbols.
- Never share passwords or authentication codes with anyone, including colleagues and IT support.
- Enable multi-factor authentication (MFA) on all business accounts where available.
- Lock their screens when leaving their workstation unattended, even briefly.
- Use a password manager approved by the Company for storing credentials.

2.2 Personnel shall immediately report any suspected account compromise, phishing attempt, or unauthorized access to IT support.

SECTION 03

Acceptable Use

3.1 Company IT resources (computers, networks, email, internet, software) are to be used primarily for business purposes. The following activities are prohibited:

- Accessing, downloading, or distributing illegal, offensive, or inappropriate content.
- Installing unauthorized software or connecting unapproved devices to Company systems.
- Circumventing security controls, firewalls, or monitoring systems.
- Using Company systems to conduct personal business activities for profit.
- Sending unsolicited bulk emails or spam from Company accounts.

3.2 Limited personal use of Company resources is permitted, provided it does not interfere with work duties, consume excessive resources, or violate this Policy.

SECTION 04

Data Handling

4.1 Personnel shall classify and handle Company and client data according to its sensitivity:

Classification	Examples	Handling Requirements
Public	Marketing materials, published documents	No special controls required
Internal	Internal memos, team documents	Share only with authorized personnel
Confidential	Client data, financial records	Encrypt in transit & at rest; need-to-know basis
Restricted	Passwords, secrets, PII	Highest protection; limited access; audit logs

4.2 Personnel shall not transfer Company or client data to personal email, personal cloud storage (Dropbox, Google Drive, iCloud), or personal devices unless expressly authorized and using Company-approved encryption.

4.3 Confidential and Restricted data shall not be discussed in public places, on public Wi-Fi, or in any forum where unauthorized parties could overhear or intercept the communication.

SECTION 05

Device and Remote Work

5.1 Personnel using Company-issued devices shall:

- Keep devices updated with the latest security patches and operating system updates.
- Enable disk encryption on all laptops and mobile devices.
- Install only software approved by the Company's IT department.
- Report lost or stolen devices to IT within 24 hours.
- Return all Company devices upon termination of employment or engagement.

5.2 Personnel working remotely shall:

- Use the Company's VPN when accessing internal systems from public or home networks.
- Avoid working in public places where screens can be viewed by unauthorized parties.
- Ensure home network security, including WPA2/WPA3 encryption and strong router passwords.
- Keep devices physically secure and never leave them unattended in public places.

SECTION 06

Incident Reporting

6.1 Personnel shall immediately report any suspected security incident, including:

- Phishing emails, suspicious attachments, or social engineering attempts.
- Lost or stolen devices containing Company data.
- Unauthorized access to Company systems or accounts.
- Accidental data disclosure or misdirected emails containing Confidential data.
- Malware infections, ransomware alerts, or unusual system behavior.

6.2 Incidents shall be reported to IT support or compliance at compliance@docree.com. Reporting in good faith will not result in disciplinary action, even if the incident was caused by user error.

SECTION 07

Consequences

7.1 Violation of this Policy may result in disciplinary action, including warnings, suspension, or termination, and may expose the individual to civil or criminal liability under applicable data protection and cybersecurity laws.

7.2 By signing this Policy, personnel acknowledge that they have read, understood, and agreed to comply with its provisions.

	Employee / Contractor	Docree Demo
Name		
Signature		

Date		

© 2026 Docree Demo. All rights reserved.

docree.
Generated at docree.com — Powered by Brokeret Solutions