



2024

JJIF BYOD (Bring Your Own Device) Policy

CONFIDENTIAL



JJIF Ju-Jitsu International Federation

JJIF Registered Office: c/o Linus Bruhin, Leutschenstrasse 9 Postfach 323, CH 8807 Freienbach, Switzerland
JJIF Headquarter: P.O. Box 110006, Abu Dhabi, UAE (Capital Tower, ADNEC Area,) mail@jjif.org

Created by

| Document owners | Role |
|-----------------|-------------------------|
| P. Schouten | Administration Director |
| | |
| | |

Document Version Management

| Version | Date | Author | Description |
|---------|------------|-------------|------------------|
| 1.0 | 10-04-2024 | P. Schouten | Initial document |
| | | | |
| | | | |

Ju-Jitsu International Federation is a proud Member of:





JJIF Ju-Jitsu International Federation

JJIF Registered Office: c/o Linus Bruhin, Leutschenstrasse 9 Postfach 323, CH 8807 Freienbach, Switzerland
JJIF Headquarter: P.O. Box 110006, Abu Dhabi, UAE (Capital Tower, ADNEC Area,) mail@jjif.org

Table of Contents

| | |
|---|----------|
| Table of Contents | 2 |
| 1. Purpose | 3 |
| 2. Scope | 3 |
| 3. Policy | 3 |
| 3.1 Device Eligibility | 3 |
| 3.2 Security Requirements | 3 |
| 3.3 Access Control | 3 |
| 3.4 Data Management | 3 |
| 3.5 Privacy | 4 |
| 3.6 Compliance with Legal and Policy Requirements | 4 |
| 3.7 Reporting | 4 |
| 3.8 Consequences of Non-Compliance | 4 |
| 3.9 Responsibility | 4 |
| 4. Agreement | 4 |
| 5. Review and Modification | 4 |
| 6. Approval and Implementation | 5 |

Ju-Jitsu International Federation is a proud Member of:





JJIF Ju-Jitsu International Federation

JJIF Registered Office: c/o Linus Bruhin, Leutschenstrasse 9 Postfach 323, CH 8807 Freienbach, Switzerland
JJIF Headquarter: P.O. Box 110006, Abu Dhabi, UAE (Capital Tower, ADNEC Area,) mail@jjif.org

1. Purpose

The purpose of this BYOD policy is to define the standards and procedures for staff members who use personal devices to access JJIF resources. This policy aims to protect the security and integrity of the federations data and technology infrastructure.

2. Scope

This policy applies to all staff, contractors, volunteers who intend to use a personal device to access JJIF networks, privacy data and systems.

3. Policy

3.1 Device Eligibility

- Only devices that meet the minimum security standards set forth by the JJIF Data Protection Officer are eligible for use.
- Devices must be no more than 5 years old and must run an up-to-date operating system.

3.2 Security Requirements

- Devices must have a secure lock screen (e.g., PIN, password, biometric).
- Devices must have encryption enabled to protect stored data.
- Devices must have the latest approved anti-virus software installed and maintained.
- Devices must be configured to receive regular updates for the operating system and installed applications.

3.3 Access Control

- Access to JJIF resources from a personal device must be through secure and approved methods such as VPN or encrypted connections.
- Staff members must use two-factor authentication where available to access JJIF networks and systems.

3.4 Data Management

- Staff members cannot store sensitive or confidential data directly on personal devices, including cloud platform, unless absolutely necessary and approved by the JJIF Data Protection Officer.
- Data stored on personal devices must be backed up regularly to a JJIF-approved storage solution. Currently this consist of Microsoft OneDrive as part of a JJIF Office 365 account of the JJIF Dropbox.





JJIF Ju-Jitsu International Federation

JJIF Registered Office: c/o Linus Bruhin, Leutschenstrasse 9 Postfach 323, CH 8807 Freienbach, Switzerland
JJIF Headquarter: P.O. Box 110006, Abu Dhabi, UAE (Capital Tower, ADNEC Area,) mail@jjif.org

- JJIF retains the right to wipe federation data from personal devices if the device is lost, stolen, or upon termination of employment.

3.5 Privacy

- JJIF recognizes the right to personal privacy and will only access or monitor data strictly related to work activities.
- Personal devices may be subject to compliance audits and security reviews as deemed necessary by the JJIF Data Protection Officer.

3.6 Compliance with Legal and Policy Requirements

- Staff members must ensure that their use of personal devices for work complies with all applicable laws and JJIF policies.
- This includes adherence to policies related to data protection and privacy laws.

3.7 Reporting

- Any security breaches, loss, or theft of devices must be reported to the JJIF Data Protection Officer immediately.

3.8 Consequences of Non-Compliance

- Non-compliance with this BYOD policy can result in disciplinary action.

3.9 Responsibility

- Employees are responsible for ensuring their device meets the requirements of this policy and for managing the security and performance of their device.

4. Agreement

All employees wishing to use their personal devices in accordance with this BYOD policy must sign an agreement indicating they understand and will adhere to these policies.

5. Review and Modification

This policy will be reviewed annually or as needed to adapt to new threats and changes in technology. Changes to this policy will be communicated to all affected personnel.





JJIF Ju-Jitsu International Federation

JJIF Registered Office: c/o Linus Bruhin, Leutschenstrasse 9 Postfach 323, CH 8807 Freienbach, Switzerland
JJIF Headquarter: P.O. Box 110006, Abu Dhabi, UAE (Capital Tower, ADNEC Area,) mail@jjif.org

6. Approval and Implementation

This policy is approved by the board of directors of the JJIF and is effective immediately.

Ju-Jitsu International Federation is a proud Member of:

