JAAS Psych Consultants – Cybersecurity Policy

Version: 1.0
Approved by: Clinical Director / Technical Lead
Effective Date: October 2024
Review Cycle: Annual or after any major security incident
Applies to: All JAAS Psych staff, psychiatrists, contractors, admin team, IT partners, and external service providers.

---

1. Purpose

This policy sets the cybersecurity standards required to protect the confidentiality, integrity, and availability of JAAS Psych's clinical systems, patient records, telehealth platforms, and business information.

It ensures compliance with:

- Australian Privacy Act 1988
- Notifiable Data Breach (NDB) Scheme
- RACGP Information Security Standards
- Australian Digital Health Agency (ADHA) cybersecurity guidelines
- Medicare requirements for telehealth and digital health
- TIS National, eScript, BP & Halaxy security requirements

JAAS Psych does **not** provide emergency services. All systems exist solely to support scheduled psychiatric care delivered via telehealth.

---

2. Scope

This policy applies to:

- All JAAS Psych psychiatrists, admin team, contractors, IT support providers (e.g., Medi IT)
- All systems: Halaxy, Best Practice, eScript, Coviu, TIS, email, SharePoint, AWS/Azure resources
- All devices: laptops, desktops, mobile devices used for clinical work

- All patient information, referral documents, NDIA reports, assessments, Medicare data, and internal correspondence
- All locations where JAAS Psych work is performed (Australia-wide, remote/home offices)

---

3. Roles & Responsibilities

3.1 Executive & Clinical Management

- Approve cybersecurity policies and budgets
- Ensure compliance with healthcare privacy laws
- Oversee incident response and risk management
- Approve access to clinical and billing systems

3.2 IT Security (Medi IT)

- Maintain and secure BP, Halaxy, SharePoint, servers/cloud systems
- Monitor logs, alerts, suspicious activity
- Enforce security patches and updates
- Implement backup, retention, and disaster recovery
- Manage MFA, VPN, encrypted email, and secure fax
- Provide cybersecurity training and reminders to staff

3.3 Psychiatrists, Admin Staff & Contractors

All JAAS Psych staff **must**:

- Use strong passwords + MFA
- Store devices securely
- Report suspicious emails or system behaviour immediately
- Handle patient information according to Privacy Act and NDB
- Use only authorised systems (BP, Halaxy, SharePoint, secure email/fax)

- Never download patient files to personal drives
- Never use public Wi-Fi without VPN

Breaches may result in disciplinary action and removal of access.

---

4. Acceptable Use Policy (AUP)

Staff must **not**:

- Install unapproved apps on work devices
- Disable antivirus/endpoint protection
- Forward patient information to personal email
- Store reports or notes on unencrypted USB drives
- Use JAAS Psych systems for unrelated business or personal gain
- Share Zoom/telehealth links outside approved workflows

Only approved clinical and admin platforms may be used for patient data.

---

5. Access Control Policy

- Access follows **least-privilege** principles
- New accounts require written approval
- MFA is **mandatory** for email, cloud, BP, Halaxy, SharePoint, VPN
- Password requirements:
    - Minimum 12 characters
    - Mix of upper/lowercase, numbers, symbols
    - No reuse
    - Change every 90 days

- Account removal must occur **within 24 hours** of off-boarding
- Access reviews every **6 months**

---

6. Data Classification & Handling

Level 1 – Highly Sensitive (Clinical)

- Psychiatric assessments
- ADHD/ASD reports
- NDIA functional impact letters
- GP referrals and Medicare information
- Internal clinical discussions
- eScripts, medication summaries

Protection:
Encryption (AES-256), MFA, restricted access, secure cloud storage only.

Level 2 – Internal

- Rosters, admin workflows, fee schedules
- Internal SOPs, triage processes
- AI chatbot knowledge base content

Level 3 – Public

- Website content
- General information sheets
- Marketing materials

---

7. Technical Security Controls

7.1 Network Security

- Secure VPN for remote access
- Firewall & intrusion monitoring
- Access only via trusted networks
- No clinical work on public Wi-Fi without VPN

7.2 Endpoint Security

- Mandatory antivirus & EDR
- Auto-lock screens after 5 minutes
- Full-disk encryption on laptops
- Device loss must be reported immediately for remote wipe

7.3 Email Security

- Advanced phishing protection
- Suspicious attachments auto-quarantined
- Secure fax for GP referrals and reports

7.4 Encryption Standards

- Data at rest: **AES-256**
- Data in transit: **TLS 1.2+**
- USB devices must be encrypted and approved

---

8. Vendor & Third-Party Security

Vendors (e.g., Halaxy, Coviu, pathology providers, SharePoint, AWS/Azure) must:

- Comply with Australian Privacy Act
- Store data within approved regions
- Provide breach notification within **24 hours**

- Sign confidentiality and data protection agreements

External contractors (including IT) are bound by the same privacy rules.

---

9. Backup & Disaster Recovery

- Daily automated backups of BP databases
- Daily Halaxy cloud backups (provider-managed)
- Secure encrypted offsite/cloud backup
- Quarterly restore testing
- RTO and RPO defined according to telehealth operations
- Backups stored separately from production systems

---

10. Incident Response Procedure

All incidents—phishing, hacking attempts, lost devices, unauthorised access—must be reported immediately.

Incident Response Steps:

1. Identify – detect and verify the threat
2. Contain – isolate systems/accounts
3. Eradicate – remove malicious components
4. Recover – restore from backup
5. Document – record incident details and actions taken
6. Notify – follow NDB requirements (serious breaches must be reported to OAIC within 72 hours)

If email compromise or fraud is suspected, staff must notify:

- JAAS Psych management
- Medi IT

- NSW Police (if required)
- ACSC cyber.gov.au

---

11. Physical Security

Although JAAS Psych operates remotely, the following controls apply:

- Work devices kept in locked storage when unattended
- No printed patient documents unless required; must be shredded securely
- Access to server rooms/cloud consoles limited to authorised IT staff
- Secure storage of laptops used for telehealth and admin work

---

12. Training & Awareness

- Mandatory cybersecurity training annually
- Phishing simulations every 3–6 months
- Additional training for handling referrals, reports, and NDIA documents
- AI chatbot/SharePoint training as required

---

13. Compliance

JAAS Psych follows:

- Australian Privacy Act 1988
- NDB Scheme
- ADHA digital health security standards
- RACGP Information Security guidelines
- Medicare telehealth requirements

- OAIC breach reporting guidelines

Internal audits conducted annually.

---

14. Enforcement

Policy violations may lead to:

- Removal of system access
- Formal warnings
- Termination of contract
- Mandatory retraining
- Legal action if patient privacy is breached

---

15. Policy Review

This policy must be:

- Reviewed annually
- Updated after major system or operational changes
- Revised following any major cybersecurity incident
- Approved by the Clinical Director and IT Security Lead

Conclusion

JAAS Psych is committed to safeguarding patient privacy, protecting clinical information, and maintaining secure telepsychiatry services Australia-wide. Ongoing training, strong cybersecurity practices, and strict adherence to laws ensure safe and reliable care delivery for all patients.