NAPS NATIONAL ACADEMY OF PROFESSIONAL STUDIES

PROVIDER ID: PRV14303 | CRICOS PROVIDER CODE: 04009C

INSTITUTE OF HIGHER EDUCATION

Cyber Hygiene Protocols for Staff

1. Password Management

- Use strong, unique passwords for each system (minimum 12 characters: mix of letters – Capital and low-case letters, numbers, symbols).
- Change passwords every 90 days or immediately if you recognize any suspicious activity.
- Do not reuse passwords across systems.
- Never share your passwords with anyone, including colleagues.
- Use multi-factor authentication (MFA) wherever possible.

2. Email and Communication Security

- Be cautious of phishing emails (eg, unexpected links, urgent requests to action or threats, emails including poor grammar, spelling errors, unfamiliar greeting and salutation, emails form unfamiliar senders, or requests for login credentials, payment information or sensitive data).
- Do not click on suspicious links or open attachments from unknown sources.
- Report suspected phishing attempts to the IT team immediately at **imssupport@naps.edu.au**
- Do not use personal email accounts for official communication or file transfers.

3. Device Security

- Lock the screen of your PC every time when leaving your desk (Windows: Windows+L; Mac: Ctrl+Cmd+Q).
- Only use NAPS-approved devices or those with up-to-date antivirus software and encryption.
- Do not install unapproved software on NAPS systems or devices.
- Keep all software and operating systems updated and patched regularly.

4. Data Handling and Storage

- Store sensitive information only on NAPS-approved systems.
- Avoid storing work documents on USBs or personal cloud accounts.
- Ensure sensitive files are encrypted or access-controlled.
- Regularly review and delete obsolete files.
- Perform regular backups ensure data can be restored in case of loss or damage.

5. Remote Access Protocols

- Use VPN and secure Wi-Fi when accessing NAPS systems remotely.
- Avoid using public Wi-Fi to access work accounts.
- Ensure personal computers are protected with firewall, antivirus, and OS security patches.
- Encrypt all data end-to-end to safeguard it in the event it is stolen, lost, or otherwise compromised.
- Implement multiple layers or steps for verification to access systems remotely and/or step-up authentication to require follow-up or re-authorization to perform specific functions.

6. Social Media and Public Representation

- Do not post screenshots of internal platforms on social media.
- Ensure all public references to NAPS are accurate and authorised.
- Avoid discussing internal systems or vulnerabilities externally.

7. Incident Reporting

- Immediately report suspicious emails, unknown file downloads, system slowdowns, data disclosures, or lost devices.
- Handle sensitive and personal information carefully
- Be thorough and provide all important details; Use the IT Incident Report Form on the staff portal.

8. Training and Awareness

- Complete mandatory Cyber Security Awareness Training annually.
- Participate in training on AI risks, data privacy, and foreign interference.
- Attend briefings by external cybersecurity experts.

9. Zero Tolerance for Non-Compliance

- Non-compliance with these protocols may result in disciplinary action under NAPS' Staff Code of Conduct. Our collective vigilance is vital to protect our systems, students, and institutional reputation.