BRUC-POL003
Barossa Regional University Campus Cyber Security Policy Addendum (under RDABGLAP Policy)

1. Purpose and Addendum

1.1. Barossa Regional University Campus (BRUC) operates under the Cybersecurity Policy and Procedure of Regional Development Australia Barossa Gawler Light Adelaide Plains (RDABGLAP) POLB010-RDA_BGLAP_Cyber_Secruity_Policy.

1.1.1. This addendum outlines out how BRUC applies that policy locally and is to be read in conjunction with the RDA BGLAP Cyber Security Policy (POLB010).

1.1.2. Where any inconsistency, ambiguity, or conflict arises between the provisions of this Addendum and the RDA BGLAP Cybersecurity policy, this Addendum prevails to the extent of the inconsistency.

1.1.3. All other provisions of the RDA BGLAP Cybersecurity policy remain in full force and effect and apply to BRUC unless expressly varied by this Addendum.

2. BRUC-Specific Scope

2.1. This Addendum applies to all cyber security risks, systems, and activities associated with the operation of the BRUC.

2.2. In addition to the scope defined in the RDA BGLAP Cybersecurity Policy, this Addendum specifically applies to:

- All BRUC employees, contractors, consultants, facilitators, volunteers and casual personnel
- Students, visiting school groups, educators, and participants attending BRUC programs or events
- Third-party service providers engaged to deliver education, technology, events, or support services on behalf of BRUC
- All information and data relating to students, visitors, program participants, and partner organisations

- All BRUC-managed or BRUC-authorised systems, including but not limited to sign-in systems, customer relationship management systems, shared devices, public-access equipment, and network services
- All devices used to access BRUC systems or data, including BRUC-owned equipment and personally owned devices authorised for work or program delivery purposes.

2.3. This Addendum recognises that BRUC operates as a public-facing education and community facility and there addresses additional cybersecurity risks associated with shared technology, temporary access, visiting users, and the collection and handling of personal and student information.

2.4. BRUC does not provide user accounts or system access to students, visiting groups, or members of the public, other than access to campus Wi-Fi and limited use of shared display or presentation systems. Any sign-in required for shared presentation or display systems must be managed by authorised BRUC staff and must not involve the sharing of personal or organisational credentials with visitors.

3. Child safety and youth data protections

3.1. All personal, education, behavioural, media, and consent-related information relating to people under the age of 18 engaged with BRUC must be treated as sensitive information and afforded enhanced protection.

3.2. Access to systems and containing information relating to young people is restricted to authorised personnel only and must be limited to the minimum level required to perform approved duties. Such access will be reviewed periodically and revoked when no longer required.

3.3. The collection, storage, use and disclosure of information relation to children and young people must comply with BRUC's Child Safe and Vulnerable Adults policies and procedures, applicable privacy obligations, and any relevant legislative requirements.

3.4. Information must not be stored on personal devices, personal email accounts, or unauthorised cloud-based services.

3.5. Photographs or video recordings may be taken to document the use of the BRUC facilities and learning environment. Images must not identify individual students

unless informed consent has been obtained and documented by the responsible education provider or BRUC, as applicable.

3.5.1. Where students are present, images should be framed to avoid capturing faces, names, or other identifying features wherever practical

3.6. Security cameras are installed at BRUC for site safety and security purposes. Footage is accessed only by authorised personnel and managed in accordance with RDA BGLAP policies and applicable privacy obligations.

3.7. Where third-party education providers deliver programs at BRUC, responsibility for student records, learning data, and reporting remains with the provider, and BRUC does not collect or manage identifiable student information beyond what is required for site safety and operational purposes.

4. Individual Level

4.1 Staff must lock computers or devices when unattended to prevent unauthorised access to information.

4.2 Staff must not share organisational login credentials or allow visitors, students, or participants to use staff accounts.

4.3 When using shared or public-access devices, staff must ensure systems are logged out, cleared of personal or sensitive information and left in a secure state after use.

4.4 Staff must take reasonable care when handling personal or student information, particularly information relating to children and young people, and must only access information required to perform their duties.

4.5 Personal or student information must not be shared externally for reporting or evaluation purposes unless it is de-identified, or the disclosure of identifiable information is required by law or formally approved.

4.6 Any suspected cyber security incident, loss of device, or unauthorised access must be promptly reported in accordance with the RDA BGLAP Cyber Security Policy.

4.7 Users of shared or public-access printers must not leave documents containing personal information unattended and must collected printed materials

4.8 BRUC is not responsible for the retention or disposal of documents printed by students or visitors.

5. Organisation Level

5.1 BRUC operates within the cyber security controls, systems, and procedures established by RDA BGLAP, including identity management, data storage and access controls.

5.2 BRUC provides free Wi-Fi for visitors and students. This Wi-Fi access is logically separated from organisational systems and does not provide access to internal RDA BGLAP networks or data.

5.3 Shared presentation and display systems at BRUC may require sign-in for operational purposes and are managed by BRUC staff.

5.4 BRUC stores organisation information and records using RDA BGLAP approved systems and does not maintain separate local servers or independent cyber security infrastructure.