Rowing New South Wales Cyber-Security Guidelines:

Security Principles:

- Use strong passwords and establish appropriate internet usage guidelines
- Identify and recognise scams:
- Verify identity of information seekers
- Never send or request personal information

Information and Data Protection:

- Every time data is used / moved it can be exposed
- Monitor information that is collected through the internet
- Use security tools to maintain data protection
- Record where information is
- Classify information into categories: Highly Confidential, Sensitive, Internal Use Only etc

Security Tools

- Anti-spyware protection. Use a current anti-spyware protection program to detect and remove spyware from your computer.
- Anti-virus protection. Ensure that your computer has an up-to-date anti-virus protection program to detect and remove viruses.
- Firewall. Utilise a firewall to prevent unauthorised users from gaining access to your computer or network.
- Operating system, browser and software updates. Keep up to date with software fixes (also known as “patches” or “security updates”).
- Use a current Web browser. The newest browsers will maximise your security.
- Use PCs and software from trusted sources. Avoid installing programs and opening unsolicited email attachments from people or organisations that you do not know. Avoid using public computers for secure transactions.
- If working from home, apply the same principles to home systems.

Mobile action

- Password protect handheld devices
- Keep operating system and applications updated
- Use security applications to protect data

Backup data and information

- Automatically back up data – weekly

P.O. Box 265, Concord West, NSW 2138
Level 1, 6A Figtree Drive, Sydney Olympic Park, Homebush Bay, NSW 2127
P +61 2 8116 9777 F +61 2 8732 1618
W www.rowingnsw.asn.au ABN 16 289 721 685

- Maintain secure storage of backups (both physical and soft copies)
- Offsite backup – maintain security during transport and storage

Control Physical Access

- Prevent access by unauthorised personnel

Secure Wifi Networks

- Secure your wifi network by password protecting access

Practices on payment cards

- Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used
- Do not record details of credit card / bank details in any case
- Isolate payment systems from other programs

Limit employee access to data information

- Do not provide any one employee access to all systems
- Should only use systems appropriate to job

Passwords

- Require employees to use unique passwords
- Usernames and passwords must not be written down and left where they could be easily found.
- Precautions must be taken to prevent a username and password being copied or overheard.
- A username and password must be changed if there is any suspicion it has been compromised or made known to another person.

Plan for data loss:

- If breached a plan of action should be in place:
- Notify law enforcement of the type of breach
- Limit the damage
- Keep members informed of breach