Australian Endurance

Riders Association Inc

AUSTRALIAN ENDURANCE RIDERS’ ASSOCIATION

AERA Digital User Access Policy

DOCUMENT CONTROL

Date	Version	Description of Revision
4 February 2023	1	Initial Version

Contents

INTRODUCTION

Purpose

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of the Australian Endurance Riders Association (AERA) and this resource must be managed with care.

As the information gathered within AERA's digital components contains personal identification information of members, day members, officials and volunteers from within the sport of endurance riding AERA must take the appropriate steps to ensure the security of this data.

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use.

Formal procedures, documented within this policy, control how access to information is granted and how such access is changed or revoked.

Scope

AERA provides managed user access to the following digital environments:

- AERASpace database
- AERA Online web hub
- AERASpace web page

These tools record member and horse data, ride results and other information pertinent to conducting and managing the sport of endurance riding in Australia.

The AERA Digital User Access policy is applied to all users of these environments. This document specifically excludes management of user access to the AERA website, which is currently controlled by the AERA Webmaster.

Definition

Access control rules and procedures are required to regulate who can access AERA's digital information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing AERA's information in any format, and on any device.

Risks

On occasion information may be disclosed or accessed without authorisation, accidentally or unlawfully. Individuals or companies, without the correct authorisation and clearance may intentionally or accidentally gain unauthorised access to personal identifying information which may adversely affect members, non-members, officials and volunteers. This policy is intended to mitigate that risk.

Non-compliance with this policy could have a significant effect on the efficient operation of the sport of endurance riding and may result in financial loss, identity theft and an inability to provide necessary services to the sport.

PASSWORDS

Passwords are the first line of defence for accessing AERA's digital systems and, combined with the User ID, helps to identify people accessing the various systems.

Generic passwords, which can be used by multiple people, are not permitted within AERA's digital systems.

Password Structure

Passwords for accessing AERA's systems must meet the following standard:

- At least 10 characters in length
- Include a capitalised character
- Include a least one numeral
- Include at least one special character

Users should avoid selecting passwords that are easily discovered or detected. Examples of weak passwords include words picked out of a dictionary, names of children and pets, or simple patterns of letters from a computer keyboard, e.g., 123456.

User IDs and passwords must never be shared with another person and should always be maintained securely.

AERA, via the AERA Database Sub-committee reserves the right to modify the password structure as it sees fit.

Password Protection

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to:

- Never reveal a password to anyone
- Never use a 'remember password' function from within the browser
- Never write passwords down or store them where they are open to theft
- Never store passwords in a computer system without encryption.
- Do not use any part of the username within the password
- Do not use a password that has been used elsewhere

A breach of these guidelines may lead to loss of access to the database.

USER ACCESS

Formal processes are implemented for the provision of access to users and covers initial registration of users, ongoing access and termination of access. Each user will be:

- Allocated access rights to the tasks required of the role they hold
- Lowest level privileges will be applied to ensure that only the tasks required for the role will be available to the user
- Unique user ids will be utilised

User access rights will be reviewed regularly to ensure that the appropriate rights are still allocated and that termination of access rights is completed where a user no longer has a role requiring access.

AERA, through the AERA Database Sub-committee, is responsible for the management and application of all access levels.

Request for User Access

A request for access to the AERA Database Subcommittee for a Division based role and for a Ride Secretary must be submitted to the AERA Database Subcommittee by the Division Association. This request will be processed and the person will be provided directly with their User ID and Password to access the database. The Division Association will be advised when access has been provided.

A single login only will be provided to users. Requests for more than one login will be denied.

Length of Access

Division based roles are granted for the period in which the person holds the Division role. Ride Secretary roles are granted for a 2 year term and are renewed following approval from the Division Association. Access to the Online Nomination System is provided for a period of 2 years.

Training

Training on the role provided (Division role and Ride Secretary) to the user will be the responsibility of the Division Association.

Training for the Online Nomination System and System Administrator roles will be the responsibility of AERA, via the AERA Database Subcommittee.

System Administrators

The AERA Database Sub-committee will allocate the System Administrator role. The only users that are authorised to hold this role are approved members of the AERA Database Sub-committee. System Administrator access will only be provided once the Sub-committee member has gained an understanding of the processes associated with the digital systems and has received the appropriate level of system training.

A maximum of 4 Sub-committee members will hold the System Administrator role to reduce risk associated with too many people holding full access to the database.

Access for System Administrators are only provided for the period in which they hold a position on the AERA Database Subcommittee. Once a person's term on the Subcommittee has ended the System Administrator access level will be removed.

Online Nomination System

Access to the Online Nomination System will be approved and provided by the AERA Database Sub-committee without reference to the Division Association with which the Ride Organiser of the ride is affiliated. The AERA Database Subcommittee is responsible for the granting of approval initially and for the renewal of access for this role.

Access Review

An annual review of access will be completed by the Division Associations in terms of the Division roles. The AERA Database Subcommittee will provide information on the Division roles to be allocated and to whom they are allocated.

As Ride Secretaries are granted a two year term this role is reviewed bi-annually. The AERA Database Subcommittee will provide information on which Ride Secretary terms will be expiring. The Division Association will provide advice on which people are to be renewed for a further two year term. There is no sunset clause on provision of Ride Secretary access.

Online Nomination System access will be reviewed every two years to determine whether renewal of access is required.

Right to Deny Access

At all times AERA, via the AERA Database Subcommittee, reserves the right to refuse to provide access to any person. This may be on the basis that the user has previously infringed this User Access Policy or for any other .

Where a user account has not been utilised for a period of 12 months or greater the AERA Database Subcommittee may disable the user's access.

Removal of Installed Database

Once a person who has held any role, including the Ride Secretary and Online Nomination roles, (either Division or AERA based) vacates that role they will immediately uninstall the AERASpace database from any laptop, device or computer on which it has been installed.

User Access Declaration

Upon logging into the AERASpace database a user will be required to acknowledge and agree to the User Access Declaration. This is displayed in a pop up window and requires electronic acknowledgement to proceed to the database. Where agreement is not provided access to the database will not be granted.

DATA USAGE/SECURITY

Data Usage

Any data contained within the AERASpace database can only be used for the specific purposes of the user's role and only for purposes associated with the sport of endurance riding in Australia. Any use of this data external to these activities is considered a breach and may result in disciplinary action being taken.

Data Security

Where an AERASpace database has been installed on a user's laptop or computer the user is responsible for ensuring that the device is securely managed at all times and that the device environment has the appropriate level of protection installed.

The database contains personal identification information that can lead to identity theft should the device on which it is installed be hacked. Any loss of data is unacceptable.

Should any unauthorised access be discovered the user will notify the AERASpace System Administrators immediately.

Should it be determined that identify theft or loss of personal data has occurred from a device owned by a user AERA may institute actions to recover any losses, monetary or otherwise, from the device owner.

POLICY COMPLIANCE

If any user is found to have breached this policy, their access will be removed immediately and they may be subject to a disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).