RAIL INDUSTRY WORKER®

RIW SYSTEM RULES

VERSION 5.0

Updated 26 April 2021

AUSTRALASIAN RAILWAY ASSOCIATION

MTA Metro Trains Australia

1. GENERAL GUIDANCE

The RIW System is the core solution to the RIW Program and provides the secure platform that houses all of the information. The purpose of these RIW System Rules is to:

- Provide RIW Participant Organisations and end users with a greater understanding of the rules that govern the RIW System and sit behind system functionality, and
- Compliment the RIW Knowledge Centre, which contains all system procedures and instructions for RIW System use.

1.1. RIW website (www.riw.net.au)

If unfamiliar with the RIW System, the RIW website contains a wealth of information and assistance with navigating the RIW System and understanding system functionality and application of these System Rules; these include:

- **RIW Knowledge Centre at https://support.riw.net.au/support/solutions/**: provides full step by step instructions for all features available in the RIW System. The RIW Knowledge Centre also contains how-to videos and system video walkthroughs to further support self-learning.
- **Service Requests**: Enables companies and cardholders to provide all the relevant information in one simple transaction, which in turn allows the RIW Service Desk to complete tasks within the RIW System. Service Requests can be accessed at https://www.riw.net.au/contact-us/request-a-service/.

2. CORE RIW SYSTEM

The RIW System can track many aspects of the cardholder's profile around readiness for work, such as job roles, competencies, employment history, along with shift/swipes times and fatigue management.

The RIW System holds comprehensive records of the cardholder's qualifications, experience and on or off-site training.

No matter how many networks, projects, sites or contractors an organisation or cardholders are involved with, the RIW System efficiently manages the required information to ensure a safe workplace.

The RIW System is designed to be used in conjunction with

- myRIW (RIW cardholder portal),
- RIW App (for online Access Controlling and Spot Checking),
- PC Card Reader, Web Card Reader or PAC Reader (for Access Controlling and Spot Checking), and
- Vircarda App (for managing the virtual RIW card).

The RIW System can be accessed at https://app.riw.net.au.

2.1. Supported browsers and operating systems

Function: Access to the RIW System and mobile applications.

System / Business Rules: In addition to the requirements listed in the table below, websites must be whitelisted if your company restricts website access and or access to the Google Play Store or Apple App Store.

Operating System	Supported Browser(s)
Microsoft Windows	Google Chrome, Microsoft Edge, Firefox
Mac OS	Safari, Google Chrome
Android	Google Chrome
iOS	Safari

System Notification: After logging into the RIW System via a web browser, the RIW System will issue a pop up notice 30 minutes after inactivity, asking the user do they wish to stay connected or exit. If no response to stay connected is received, the user will be automatically logged out after an additional 5 minutes.

2.2. Cards and swiping cardholder and visitors

There are five methods that can be used to swipe/read a physical or virtual RIW card or visitor pass:

1. Via the dedicated RIW App – Android mobile (NFC or QR versions),
2. Via the dedicated RIW App – iOS mobile,
3. Via the PC Card Reader software and a USB connected card reader or QR Code Gun,
4. Via the Web Card Reader, and
5. Via the PAC Reader (i.e. turnstiles).

Software and hardware requirements for using these methods are described below.

2.2.1. Card checker key feature comparison

Function: Applications that can be used to swipe/read a physical or virtual RIW card and visitor pass (Key features are compared in the table below).

Feature	RIW App – Android	RIW App - iPhone	PC Card Reader	Web Card Reader	PAC Reader
Card checker functionality	✓	✓	✓	✓	✖
Spot checker role	✓	✓	✓	✓	✖
Team functionality	✓	✓	✖	✖	✖
Change location	✓	✓	✓	✓	✖
View location requirements	✓	✓	✖	✓	✖
Swipe card using QR code	✓	✓	✖	✓	✖
Swipe card using QR scanner	✖	✖	✓	✓	✖
Swipe cards using NFC	✓[1]	✖	✓	✖	✓
Lookup cardholder (forgotten card)	✓	✓	✓	✓	✖
Lookup visitor (forgotten pass)	✓	✓	✓	✖	✖
View swipe history	✓[3]	✓[3]	✓[4]	✓[2]	✖
View competency award history	✖	✖	✖	✓[2]	✖
View spot check history	✖	✖	✖	✓[2]	✖
Award competencies	✓	✓	✓	✓	✖
Installation required	✓	✓	✓	✖	✓
Target screen size	Mobile phone	Mobile phone	PC	Tablet, PC, mobile phone	Nil
Compatible operating systems	Android	iOS	Windows	Windows, Mac OS, iOS, Android	Windows

System / Business Rules: In addition to the functional comparisons, the additional rules include:

1. NFC is only available on Android devices and PC Card Readers supporting NFC.
2. Web card reader – displayed history is limited to 12 hours whilst user is logged in, even if browser window is closed.
3. Mobile app – swipe history is retained until the team is swiped out.
4. PC Card Reader – swipe history is removed as soon as user navigates away from screen.

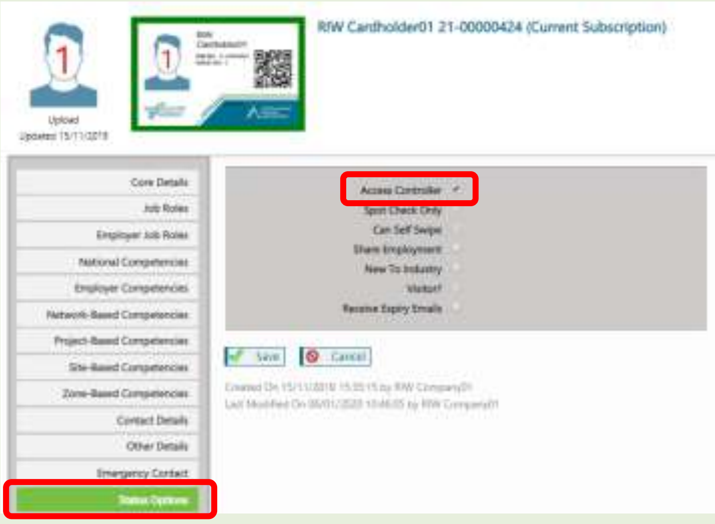
System Notification: None.

2.2.2. The RIW app (Android or iPhone)

Function: Enabling Access Controllers and Spot Checkers to use the RIW app.

System / Business Rules: The system requirements enabling the RIW app on a smart device are as follows:

- IOS App: Requires iOS 9.0 or above, and
- Android App: Requires Android 5 or above.
- Spot Checker and/or Access Controller tick box must be selected from **Status Options** within the cardholder's profile as shown below.



RIW Cardholder01 21-00000424 (Current Subscription)

Access Controller ✓
Spot Check Only ○
Can Self Swipe ○
Share Employment ○
New To Industry ○
Visitor? ○
Receive Expiry Emails ○

Created On 15/11/2018 15:55:15 by RIW Company01
Last Modified On 08/01/2020 10:46:05 by RIW Company01

- The RIW app automatically logs the Access Controller and Spot Checker out when the app is closed on the mobile device. Whilst the app is open, it will remain open, as there is no time limit for the app to automatically log either user out.
- Access Controllers and Spot Checkers must authenticate their RIW app details after:
  - The RIW app has been updated,
  - The Access Controllers and Spot Checkers logs out (**Note:** If it's the same user then no re-authentication is required but the Access Controllers or Spot Checkers must present card to log back in), or
  - You change mobile devices.

System Notification: None.

2.2.3. The Vircarda app

Function: Enabling cardholders to access their virtual card using the Vircarda app.

System / Business Rules:

- Minimum system requirements:
  - IOS App: Requires iOS 10 or above, or

- Android App: Requires Android 4.4 or above.

- The app can be downloaded from the relevant App store. Refer to https://www.riw.net.au/download-the-apps/.
- Vircarda specific rules include:
  - The Virtual Card (tick box) must be selected in the **Cards** tab within the RIW System in order to request the virtual card.
  - On receipt of the email or SMS, the cardholder clicks on the link.
  - The Vircarda app must then be downloaded and installed onto the cardholder's mobile device, the cardholder can now register their account on Vircarda, either via the link received in the SMS or email or manually.
  - From the device, click on the link in the SMS or email and Vircarda will be launched automatically, populating the required fields with the Registration Number and PIN contained in the communication. **Note:** If manually entering the required fields, the scheme prefix is 'RIW'.
  - On the next screen, Account Registration, the email and mobile number associated with your RIW record will be populated on the form, choose and type in a Password for the account, following the protocol shown.
  - If necessary, scroll to the bottom of the screen, where a link to the Terms and Conditions is provided. These should be read and if satisfied, tick the checkbox provided to confirm agreement. Next, click Create Account to complete the registration process.
  - If the cardholder's physical card is cancelled, this will also cancel their virtual card until such time as a new physical card is ordered. Once requested, the virtual card is reactivated, which allows the cardholder to continue to work.

System Notification: The RIW System sends details of the virtual card to the cardholder via SMS or email; if via email, the email will be titled **Your RIW Virtual Card.**

2.2.4. Reactivating Vircarda on a new device

Function: Enable cardholders to reaccess their virtual card using the Vircarda app.

System / Business Rules:

- Minimum system requirements:
  - As above in sections 2.2.3.
- The app can be downloaded from the relevant App store. Refer to https://www.riw.net.au/download-the-apps/.
- Vircarda specific rules include:
  - As above in sections 2.2.3.
- **Note:** The cardholder must contact the Service Desk and request their Vircarda account be unlinked

System Notification: As above in sections 2.2.3.

2.2.5. PC card reader

Function: Enabling the PC Card Reader.

System / Business Rule:

- Hardware requirements:
  - Windows compatible computer / laptop,
  - USB port,
  - Internet connectivity,
  - PC Card Reader,
    - Identive uTrust 3700 F Contactless
    - Identive SCM SCL3711, USB 13.56 Mhz ISO 14443, Mifare, Felica Reader
  - IOS App: Requires iOS 10 or above, and
  - Android App: Requires Android 4.4 or above.
- Software system must be Windows 7 or above
- Internet Browser
  - Microsoft Edge v17 or above (recommended),
  - Google Chrome v72 or above (recommended),
  - Internet Explorer v11 or above,
  - Firefox v65 or above,
  - Safari v12 or above, and
  - Windows compatible computer / laptop.
- Software and drivers
  - PC Card Reader Software
    - https://app.riw.net.au/Sync/Home/PCCardConnector
  - PC Card Reader Drivers
    - Identiv uTrust 3700F - https://support.identiv.com/3700f/
    - Identiv SLC3711 USB - https://support.identiv.com/scl3711/
  - Windows compatible computer / laptop
- Once the PC card reader is operational, the Access Controller's RIW card must be scanned to authenticate as per the RIW app, the relevant Network, Project and Site must also be selected. The PC card reader functions like the RIW app on a smart device.

System Notification:

- None.

2.2.6. Web card reader

Function: Enabling the Web Card Reader.

System / Business Rule:

- Software Requirements:
    - Microsoft Windows: Google Chrome, Microsoft edge & Firefox
    - Mac OS: Safari and Google Chrome
    - Android: Google Chrome
    - iOS version 10 and above: Safari
- The cardholder must be an Access Controller or Spot Checker to use the Web Card Reader function.
- Access is via the existing built-in camera on the laptop or a QR scanner gun if one is attached to the laptop. Like the RIW app, scanning the Access Controller or Spot Checkers card to gain an authentication code must be entered before proceeding.
- Once the Network, Project and Site are selected, the Web Card now functions like the RIW app on a smart device.

System Notification:

- An authentication message will be sent via email or SMS once the Access Controller or Spot Checker's card is scanned.

2.2.7. PAC reader

Function: Enabling Physical Access Control (PAC) Reader.

System / Business Rule:

- Once the turnstile and reader are powered up, the reader must be aligned to the site within the RIW System. This is done by the Service Desk via the **Administration** tab and **PAC Readers** link.
- Once the PAC reader is aligned to the Project and Site, access requirements can be set up via the **Administration** tab and **Site** link by those users with the permission to do so; this includes, Employer Administrator and the Advanced Project Administrator, Project Administrator and Site Administrator where that **Site** resides.

System Notification:

- None.

3. TIME ZONES

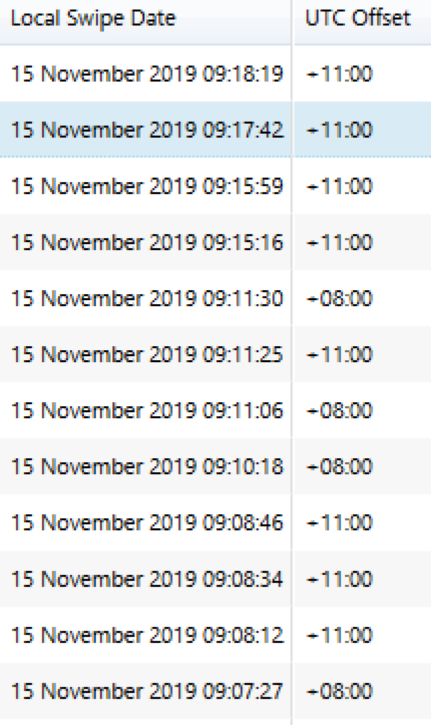
3.1. Time sensitive information

Function: Processing of time sensitive information including:

- Swipes' i.e. spot checks, team swipe in's, awarding RIW App competencies, etc., activity recorded via the mobile apps or PC card reader function; and
- Visitor Pass validity periods.

System / Business Rules: The time and date information is displayed in the RIW System with the time zone that it was recorded in and the UTC offset.

System Notification: None.



Local Swipe Date	UTC Offset
15 November 2019 09:18:19	+11:00
15 November 2019 09:17:42	+11:00
15 November 2019 09:15:59	+11:00
15 November 2019 09:15:16	+11:00
15 November 2019 09:11:30	+08:00
15 November 2019 09:11:25	+11:00
15 November 2019 09:11:06	+08:00
15 November 2019 09:10:18	+08:00
15 November 2019 09:08:46	+11:00
15 November 2019 09:08:34	+11:00
15 November 2019 09:08:12	+11:00
15 November 2019 09:07:27	+08:00

3.2. Date sensitive information

Function: Processing of date sensitive information including:

- Competency expiries
- Medical expiries
- Subscription expiries
- Employment/Association start/end dates
- Blocks
- Allocated items

System / Business Rules:

- Date sensitive data listed above resets at two minutes past midnight (0002/12:02am) AEST (Australian Eastern Standard Time) irrespective of the time zone in which the record/data is added. The only difference to that is company subscription which is triggered at midnight (0000/12:00am) UTC (Universal Time Clock) which equates to 1000/10:00am AEST.

System Notification: None.

4. MYRIW

4.1. Enabling myRIW

Function: Enabling cardholders to use their myRIW.

System / Business Rules:

- A cardholder must have a myRIW account in order to work within the RIW Program.
- A cardholder user can access myRIW by either:
  - Direct website https://app.riw.net.au/MySkillGuard/Account/LogOn, or
  - Via the RIW website at https://riw.net.au, or
  - Via the link sent from the system when the cardholder's profile is saved after creation.
- After logging on, users stay connected to myRIW. No pop-up notifications are issued by the RIW System to remind the user to disconnect or stay connected.

System Notification:

- Once the cardholder's profile has been saved, the system sends a **myRIW Registration Email** to the cardholder's email address inviting them to create their myRIW account.
- All employment and association requests reside in the **Employers & Association** tab.

4.2. Cardholders updating their details within myRIW

Function: Updating cardholders details via myRIW.

System / Business Rules:

- A cardholder can only update their own mobile and email address via myRIW.
- A cardholder can send a request to the primary employer administrator who is listed as the primary contact to update their details other than mobile and email address.

System Notification:

- A update request notification email will be sent to the primary employer administrator who is listed as the primary contact.

4.3. Permission Access Agreement Rejection

Function: System status when the Permission Access Agreement (PAA) is rejected by the cardholder.

System / Business Rules:

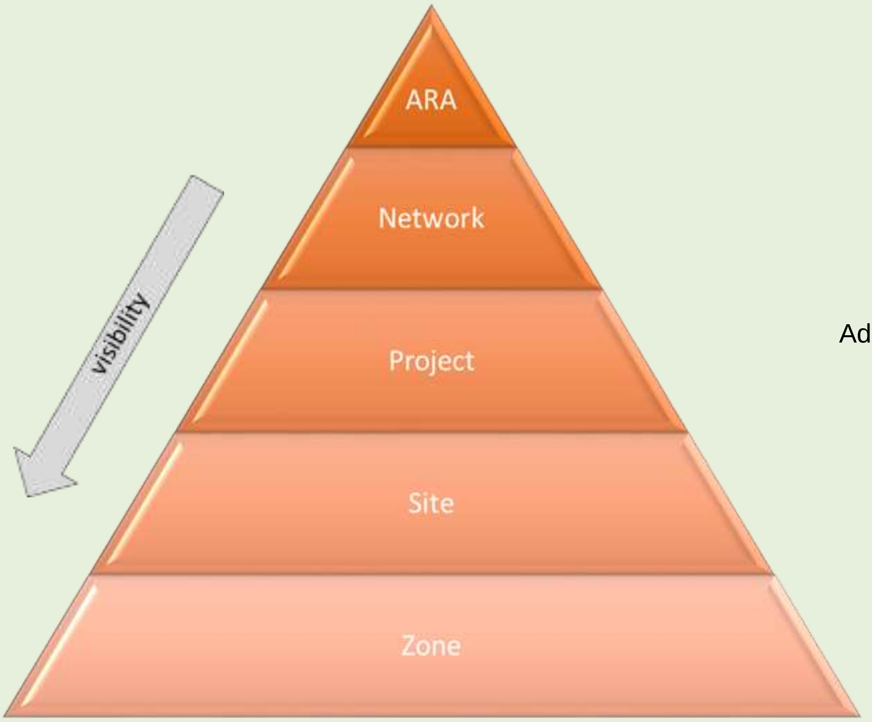
- The PAA must be accepted for the cardholder to access their myRIW account.
- Employment requests can only be accepted via the cardholder's myRIW account.
- PAA approvals can be monitored by the Employer Administrator from the **Home** dashboard.
- Rejecting the PAA means the cardholders profile is immediately deleted from the RIW System.
- The initial cardholder's profile is deleted after 28 days if the cardholder does not respond to the PAA.

System Notification:

- The Employer Administrator is sent a **Person Pending Participant Acceptance Agreement Rejected** email informing them that the cardholder has rejected the PAA.
- After rejecting the PAA, the Employer Administrator is sent a **Person Pending Participant Acceptance Agreement Consent Deleted** email, informing the cardholder that all data associated with the cardholder has been deleted and that if the cardholder wishes to re-join the RIW Program, a new profile will need to be created.

5. SYSTEM PERMISSION HIERARCHY

The RIW System has been designed around privacy, ensuring the highest level of security is maintained and that permission is sought from the RIW cardholders before their information is shared with the RIW Program. Different levels of permission access ensure a greater focus on privacy and security. Permissions are cascaded down, meaning that administrators only have visibility of their permission level or lower, and cannot search the system for information that they don't have permission to view.



Network Operator

↓

Employer Administrator
Advanced Project Administrator
Project Administrator

↓

Site Administrator

Network Operators including Network Operator – Read only: Network Operators have view rights to all RIW cardholders who are active on their network. Network Operators are able to edit profiles to place blocks in the event of an investigation or incident.

Employer Administrators includes – Employer Administrators, Employer Administrators - No Payment, Employer Administrators – Read Only and Premium Functionality Employer Administrators: Employer Administrators are able to view and manage their workforce, including projects that have been assigned to them as the Contractor in Charge.

Advanced Project Administrators: Permission designed to assist Employer Administrators with managing their own employees and the workforce of the project.

Project Administrators: Permission designed to manage the workforce specifically on a project.

Site Administrators: Permission designed to manage the workforce specifically on a site within a project.

5.1. RIW System Permissions Matrix

The permissions associated with what each RIW System User permission can do is located at section **Error! Reference source not found.** and online via the following hyperlink. Where the creation of a user permission has a system rule and or a system notification, these are explained in the following paragraphs.

5.2. Network Operator Permission Creation

Function: Creation of a new Network Operator.

System / Business Rules:

- New Network Operators are created via a Service Desk request and must be approved by the National Rail Industry Worker Governance Committee (NRIWGC).
- All users logging in for the first time must read and accept the **System Access Rules** and click the **Agree** button before access is granted.

System Notification:

- A **RIW Registration Email** is sent to the nominated user after the Service Desk has created the account. The user has 24 hours to activate the account and set the password via the link provided in the email. The link will expire if the link has been used (registration is completed).
- After 24 hours the user can click on the forgotten password at the login page or ask the permission creator to resend the link.

5.3. Network Operator – Read Only – Permission Creation

Function: Creation of a new Network Operator – Read Only permission.

System / Business Rules:

- Network Operator – Read Only permissions are created (and deleted) by a full access Network Operator administrator via the **My account Tab** and the **Manage Colleague Logins** shortcut.
- All users logging in for the first time must read and accept the **System Access Rules** and click the **Agree** button before access is granted.

System Notification:

- A **RIW Registration Email** is sent to the nominated user after the permission has been created. The user has a 24-hour window to activate the account and set the password via the link provided in the email. The link will expire if the link has been used (registration is completed).
- After the 24-hour activation window, the user can click on the forgotten password option on the login page or ask the permission creator to resend the link.

5.4. Employer Administrator Permission Creation

Function: Creation of a new Employer Administrator permission.

System / Business Rules:

- The initial Employer Administrator user permission is created as part of company setup.
- Once setup, other Employer Administrator permissions are created (and deleted) by a full access Employer Administrators via **My account Tab** and the **Manage Colleague Logins** shortcut on the dashboard.
- Full access Employer Administrators can issue other Employer Administrator permissions and all other lower hierarchy permissions via **My account Tab** and the **Manage Colleague Logins** shortcut on the dashboard.
- All users logging in for the first time must read and accept the **System Access Rules** and click the **Agree** button before access is granted.

System Notification:

- A **RIW Registration Email** is sent to the nominated user after the permission has been created. The user has a 24-hour window to activate the account and set the password via the link provided in the email. The link will expire if the link has been used (registration is completed).
- After the 24-hour activation window, the user can click on the forgotten password option on the login page or ask the permission creator to resend the link.

5.5. Employer Administrator – No Payment – Permission Creation

Function: Creation of a new Employer Administrator – No Payment permission.

System / Business Rules:

- New Employer Administrator – No Payment permission is created by full access Employer Administrator via **My account Tab** and the **Manage Colleague Logins** shortcut on the dashboard.
- Employer Administrator – No Payment cannot create any other Employer Administrator users.
- All users logging in for the first time must read and accept the **System Access Rules** and click the **Agree** button before access is granted.

System Notification:

- A **RIW Registration Email** is sent to the nominated user after the permission has been created. The user has a 24-hour window to activate the account and set the password via the link provided in the email. The link will expire if the link has been used (registration is completed).
- After the 24-hour activation window, the user can click on the forgotten password option on the login page or ask the permission creator to resend the link.

5.6. Employer Administrator – Read Only – Permission Creation

Function: Creation of a new Employer Administrator – Read Only permission.

System / Business Rules:

- New Employer Administrator – Read Only permissions are created by a full access Employer Administrator via **My account Tab** and the **Manage Colleague Logins** shortcut on the dashboard.
- Employer Administrator – Read only cannot create any other Employer Administrator users.
- All users logging in for the first time must read and accept the **System Access Rules** and click the **Agree** button before access is granted.

System Notification:

- A **RIW Registration Email** is sent to the nominated user after the permission has been created. The user has a 24-hour window to activate the account and set the password via the link provided in the email. The link will expire if the link has been used (registration is completed).
- After the 24-hour activation window, the user can click on the forgotten password option on the login page or ask the permission creator to resend the link.

5.7. Advanced Project Administrator Permission Creation

Function: Creation of a new Advanced Project Administrator permission.

System / Business Rules:

- Advanced Project Administrator permission is created by a full access Employer Administrator via **My account Tab** and the **Manage Colleague Logins** shortcut on the dashboard, providing the company has Premium functionality enabled and is selected as the Contractor in Charge for a Project.
- If the company is selected as the Contractor in Charge for multiple projects with the same or different Network Operator, separate Advanced Project Administrator permissions must be set up for any given user.
- The Advanced Project Administrator permission ends when the project ends.
- All users logging in for the first time must read and accept the **System Access Rules** and click the **Agree** button before access is granted.

System Notification:

- A **RIW Registration Email** is sent to the nominated user after the permission has been created. The user has a 24-hour window to activate the account and set the password via the link provided in the email. The link will expire if the link has been used (registration is completed).
- After the 24-hour activation window, the user can click on the forgotten password option on the login page or ask the permission creator to resend the link.

5.8. Project Administrator Permission Creation

Function: Creation of a new Project Administrator permission.

System / Business Rules:

- New Project Administrators are created by the full access Employer Administrator or Advanced Project Administrator via **My account Tab** and the **Manage Colleague Logins** shortcut on the dashboard.
- All users logging in for the first time must read and accept the **System Access Rules** and click the **Agree** button before access is granted.

System Notification:

- A **RIW Registration Email** is sent to the nominated user after the permission has been created. The user has a 24-hour window to activate the account and set the password via the link provided in the email. The link will expire if the link has been used (registration is completed).
- After the 24-hour activation window, the user can click on the forgotten password option on the login page or ask the permission creator to resend the link.

5.9. Site Administrator Permission Creation

Function: Creation of a new Site Administrator permission.

System / Business Rules:

- New Site Administrator permissions are created by either the full access Employer Administrator, Advanced Project Administrator or Project Administrator via **My account Tab** and the **Manage Colleague Logins** shortcut on the dashboard.
- All users logging in for the first time must read and accept the **System Access Rules** and click the **Agree** button before access is granted.

System Notification:

- A **RIW Registration Email** is sent to the nominated user after the permission has been created. The user has a 24-hour window to activate the account and set the password via the link provided in the email. The link will expire if the link has been used (registration is completed).
- After the 24-hour activation window, the user can click on the forgotten password option on the login page or ask the permission creator to resend the link.

6. COMPANY REGISTRATION

6.1. Company Registration

Function: Companies registering in the RIW System.

System / Business Rules:

- Initial company registration is completed via the **Company Registration** link on the www.app.riw.net.au home page.
- Once submitted, the Service Desk undertakes checks to ensure the applicant has the authority to use the ABN. Once verified, approving the application triggers a system generated email with a username and initial password to be sent to the registered user.

System Notification:

- An **RIW Registration Email** is sent after the Service Desk has approved the company creation. This provides the primary user with a link (active for 24 hours. The link will expire if the link has been used (registration is completed).
- After 24 hours the user can click on the forgotten password at the login page or ask the Service Desk to resend the link.

7. PASSWORD RESET

Once the account is active, system users have five attempts to enter their password correctly. Failure to do so will result in the user being locked out of their account. Once the account is locked, unlocking can be done by contacting the user who created the account or the Service Desk. The following paragraphs provide additional guidance as to who can reset passwords once user account are locked.

Network Operator user permissions can reset the following user permissions within their organisation:

- Other Network Operator users, and
- Network Operator – Read Only users.

Employer Administrator user permissions can reset the following permissions within their organisation:

- Other Employer Administrator users,
- Employer Administrator – Read Only users,
- Employer Administrator – No Payment users,
- Advanced Project Administrator users,
- Project Administrators users, and
- Site Administrator users.

Advanced Project Administrator permissions can reset the following permissions within their organisation:

- Other Advance Project Administrator users,
- Project Administrators, and
- Site Administrator.

Employer Administrator – Read Only, Employer Administrator – No Payment and Site Administrator permissions cannot reset any passwords for other permissions.

Resetting the password for Registered Training Organisations and Authorised Health Professionals, when the account is locked, can only be done via the Service Desk

Any time before the account is locked, a user can click on **Forgotten Password** link to reset their password.

8. CARDHOLDER ACTIVITIES

8.1. Creation of Initial Cardholder Profile

Function: Creating a cardholder's initial profile.

System / Business Rule:

- Employer Administrator's and Advance Project Administrator's can create a new person can do so by clicking on **Add New person** or **Add New Person icon.**
  - All mandatory fields must be completed.
  - The **Check for Duplicates** button must be clicked to confirm a worker is unique before proceeding. Duplicate workers must be resolved via the Service Desk.
  - A photo of the worker must be uploaded (and compliant with the requirements provided on the upload pop up).
  - Cardholder profile must be saved before the employment request will be sent by the system.
- Profile updates, competencies, job roles etc cannot occur until the cardholder has accepted the employment request via their myRIW.
- Once the profile is complete, changing a name or date of birth can only occur via the Service Desk.

System Notification:

- The Administrator can monitor the on boarding process of new or existing cardholders via the **Employment Approval** on the main dashboard.

8.2. ID Check

Function: Cardholder ID check request.

System / Business Rules:

- **Request ID Check** within the system cannot commence until the cardholder has accepted the employment request (via their myRIW) and key information has been added to the cardholder's profile.
- Once the cardholder's profile is complete, payment must be made before the ID check is initiated.
- Once the ID check is complete, core details can only be changed via a Service Desk request, ie. marriage or changing their name by deed poll.
- Examples of acceptable identification documents can be found at the following link. https://www.riw.net.au/wp-content/themes/MTAThemeV1/QuickGuides/Quick%20Guide%20-%20Acceptable%20identification%20documents.pdf

System Notification:

- The cardholder is sent an **Application Form Invite** email from Veritas asking the cardholder to login and commence uploading documents.
- Once the cardholder commences the ID check, the Employer Administrator is sent a **RIW ID Check – Status Update** email confirming the cardholder has been sent an email to commence the ID check.

- Once the cardholder commences the ID check, the Employer Administrator is sent a **RIW ID Check – Status Update** email confirming the ID Check is Pending, indicating the cardholder has started the process.
- Once the cardholder completes the uploading of documents, the Employer Administrator is sent a **RIW ID Check – Status Update** email confirming the ID Check is with **Pending Veritas**, indicating the ID check is with Veritas to confirm the identity of the cardholder.
- When Veritas have confirmed the ID check, the Employer Administrator is sent a **RIW ID Check – Status Update** email – **ID Check Successful**, indicating the cardholder's ID has been verified.
- If the ID check was unsuccessful, the Employer Administrator is sent a **RIW ID Check – Status Update** email – **ID Check Unsuccessful** – with the reason why.
- If the cardholder's details entered into the RIW System do not match the evidence provided by the worker, the Employer Administrator and the cardholder is sent a **RIW ID Check – Status Update** email – **Login Failed**, indicating a mismatch in the cardholder's records. The email alerts the Employer Administrator to check the cardholder's details, pay again and resubmit.

8.3. Ordering Physical Cards

Function: Ordering a cardholder's physical card.

System / Business Rules:

- The system requires the following to be valid before a card can be requested:
  - A current and valid photo,
  - A valid name,
  - A verified ID check, and
  - An employer.
- By default, cards are sent to the primary company address. If multiple work locations were attached to the cardholder's profile, one of these can be selected.
- The **Deliver Card to Worker** tick box must be ticked for the card to be sent to the worker's home address.
- Employer Administrators and Advanced Project Administrators can monitor the status of a cardholder's physical card and virtual card via the **Card Status** shortcut from the home page.

System Notification:

- Once payment has been made a **RIW Order Confirmation** email is sent the administrator responsible for ordering the card with the invoice attached.

8.4. Ordering a Virtual Card

Function: Ordering a cardholder's physical card.

System / Business Rules:

- The system requires the following to be valid before a card can be requested:
    - A current and valid photo,
    - A valid name,
    - A verified ID check, and
    - An employer.
- By default, cards are sent to the primary company address. If multiple work locations were attached to the cardholder's profile, one of these can be selected.
- The **Deliver Card to Worker** tick box must be ticked for the card to be sent to the worker's home address.
- Employer Administrators and Advanced Project Administrators can monitor the status of a cardholder's physical card and virtual card via the **Card Status** shortcut from the home page.

System Notification:

- Once payment has been made a **RIW Order Confirmation** email is sent the administrator responsible for ordering the card with the invoice attached.

8.5. Cardholder Subscriptions

Function: Annual cardholder subscription. This function includes the following:

- Annual subscription – covers ongoing maintenance of the cardholder's active profile,
- Five-year subscription – covers ordering of a new physical card and maintenance of the cardholder's active profile, and
- Ten-year subscription – covers ordering of a new physical card, ID check of the updated photo and maintenance of the cardholder's active profile.

System / Business Rules:

- Failure to pay will result in the Employer Administrator's continuing to see the cardholder via the People's tab and able to pay the annual cardholder subscription.
- The cardholder will have no authority to work and therefore cannot be swiped in by the Access Controller.
- When the cardholder is checked by the Spot Checker, the app will indicate the cardholder's subscription has expired.
- **Worker Subscription has lapsed for less than a year within a five-year cycle**
    - When the next subscription date is in the past and less than a year ago and the next 5-year subscription renewal is in the future, when the subscription is paid, the next subscription date is calculated to end as if the subscription had been ongoing without a lapse (to maintain alignment across the system).

    - Example.
        - Subscription due: 17 Jan 20
        - Current date: 17 Aug 20
        - Subscription paid: 17 Aug 20
        - Next subscription due: 17 Jan 21
        - **Note.** The payment made pays the remaining 5-months of current cycle to maintain alignment across the system. Payment does not change the next subscription date.
- **Worker Subscription has lapsed for more than a year within a five-year cycle**
    - When the next subscription date is in the past and over a year ago and the next 5-year subscription is in the future, when the subscription is paid, the next subscription date is calculated to end as if the subscription had been ongoing without a lapse (to maintain alignment across the system).
    - Example.
        - Subscription due: 17 Jan 19
        - Current date: 17 Aug 20
        - Subscription paid: 17 Aug 20
        - Next subscription due: 17 Jan 21
        - **Note.** The payment made pays the remaining 5-months of current cycle to maintain alignment across the system. The cardholder is not required to pay for the year missed 17 Jan 19 to 17 Jan 20. Payment does not change the next subscription date.
- **Work Subscription has lapsed and the Next Major Subscription Date is in the past**
    - Once a new subscription is paid, the cycle start date is cleared/reset back to the date of payment, and the next major subscription will be five years from then.

System Notification:

- A **RIW Individual Subscription Expiring** email will be sent to the cardholder and Employer Administrator at 4 weeks, 1 week and day the renewal is due.
- A **RIW Individual Subscription Expired** email will be sent to the cardholder and Employer Administrator on the day of expiry informing the cardholder they have no authority to work.
- A **RIW Order confirmation** email is sent once payment is made via PayPal or POA with the invoice attached.

8.6. Awarding Job Roles and Competencies for Cardholders

Function: Awarding job roles and competencies to cardholders.

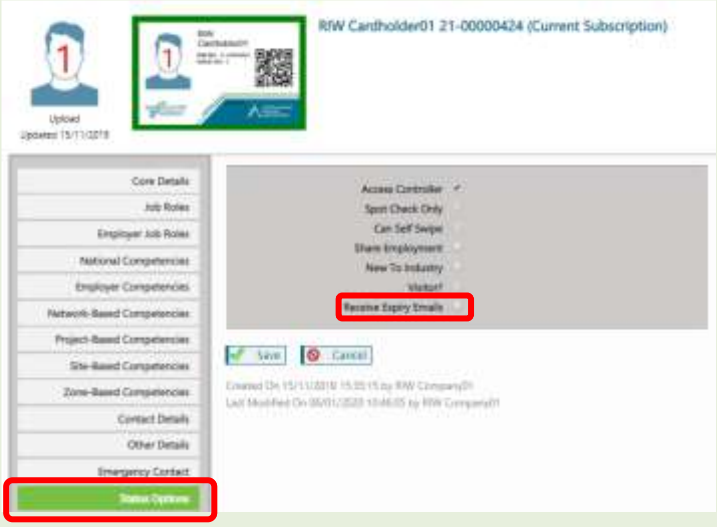
System / Business Rules:

- Network, National, Project and Site Competencies can be added by the Employer Administrator and Advanced Project Administrator to Primary, Secondary, Associated and Linked cardholders.
- Employer Administrator and Advanced Project Administrator of companies with premium functionality can also add employer competencies to Primary, Secondary, Associated and Linked cardholders.

- Roles can only be awarded by the Primary Employer.
- Assessed job roles cannot be submitted unless all competencies have been submitted and verified.
- Changing any assessed competency within an assessable job role will render the role invalid and require the role to be reassessed.

System Notification:

- Employer Administrators receive the following system generated emails:
  - Assessable Job Roles:
    - The Employer Administrator is sent a **Job Role sent for Assessment** email indicating the role has been sent to the nominated assessor.
    - The Employer Administrator is sent a **Job Role Assessment Rejected** email indicating the submitted job role was rejected by the assessor; the email contains the name of the role.
    - The Employer Administrator is sent a **Job Role Assessment Approved** email indicating the submitted job role was approved by the assessor; the email contains the name of the role.
  - Competencies Expiring
    - Expiries are managed via the expiries tab within the RIW System.
  - Competencies Rejected
    - The Employer Administrator is sent a **Competency Rejected** email indicating the competency was rejected by the Service Desk; the email contains the name of the competency but not the reason why.
- If the Employer Administrator ticks the **Receive Expiry Emails**, within **Status Options** of the cardholder's profile, the cardholder will also receive system generated emails for all transactions where expiry emails exist.



Access Controller ☑
Spot Check Only □
Can Self Swipe □
Share Employment □
New To Industry □
Visitor? □
Receive Expiry Emails □

Created On 15/11/2018 15:55:15 by RIW Company01
Last Modified On 08/01/2020 10:46:05 by RIW Company01

8.7. Cardholder Unfit Medical

Function: Medical status changes.

System / Business Rules:

- Refer section 14.1 for further details on rules associated with medical results recorded by the AHP.

System Notification:

- As a result of an AHP applying an unfit status, the Employer Administrator is sent an **URGENT: Unfit Medical Result – cardholder name – cardholder number** email confirming the cardholder has been deemed unfit and therefore any role requiring that medical will no longer be valid.
- **Note:** If the cardholder holds multiple medicals the email does not indicate which of the medicals changed from fit to unfit. The Employer Administrator would need to log in to the system to determine which certificate had changed state.

8.8. Cardholder D&A Failure

Function: Administration of D&A Failures.

System / Business Rules:

- Refer section 14.2 for further details on rules associated with D&A results recorded by the AHP.
- Any failed D&A result recorded via an AHP results in a National Block. This block is a sum of individual network blocks which enables those Network Operators with a second chance/rehabilitation program to lift the block on their network with the block still remaining on the other networks.

System Notification:

- If the outcome from a D&A screen was a fail, the Employer Administrator is sent an **Urgent: D&A Test Positive Fail** email confirming the cardholder has failed the screen and is banned from working on all rail networks.
- **Note:** D&A tests conducted via random, post incident or show cause, are administered via the blocks and suspensions process and not via the AHP user permission.

9. ROLES & COMPETENCIES

9.1. National and Network Job Roles and Competencies

Function: Setting up new or amending job roles and competencies.

System / Business Rules:

- National and Network role and competencies are set up or amended via a Service Desk request.
- National job roles and competencies must be approved by the NRIWGC.

System Notification:

- None.

9.2. Employer Job Roles

Function: Setting up new or amending employer job roles.

System / Business Rules:

- Employer job roles can be set up by the Employer Administrator with access to premium employer functionality.
- These roles are setup by clicking on the **Employer Job Roles** shortcut and completing the system template.
- Key fields include:
  - Name – self explanatory.
  - Is Safety Critical – identifies if the role is safety critical which can be used with workforce management and specific reporting.
  - Medical Level – a medical level can be selected if the competency requires one. If not, user should select **No medical required**.
  - Requires Drugs and Alcohol Test Pass – the role requires a successful D&A test.
  - Is Active – If Active checkbox is ticked the role is active and can be selected. If a Job Role is made inactive (i.e. the Is Active checkbox is deselected) this will prevent it from being assigned to cardholders, and being displayed. This includes preventing it from being displayed on any cardholder to which it was previously assigned (e.g. during swipe in activities). If re-activated later, the Job Role will again appear as assigned to these cardholders unless an end date for the role has been manually added to their record.
- Once the role is created, the Employer Administrator is required to determine what the competencies requirements of the job role are via the **Edit the Employer Job Role** from the job role summary screen.

System Notification:

- None.

9.3. Employer Competencies

Function: Setting up new or amending employer competencies.

System / Business Rules:

- Employer competencies can be set up by the Employer Administrator with access to premium employer functionality.
- These competencies are setup by clicking on the **Employer Competencies** shortcut and completing the system template.
- Key fields include:
  - Category – drop down fields exist to categorise the competency.
  - Medical Level – a medical level can be selected if the competency requires one. If not, user should select **No medical required**.
  - Awardable – this tick box must be selected to enable the competency to be awardable.
  - Always Award New – If the **Always Award New** checkbox is ticked then, if the Competency has previously been awarded to the cardholder, when it is awarded again (re-certification) it will override the older instance with the most up-to-date expiry date rather than creating a new instance of the Competency. If this box is left un-ticked, when it is awarded, the older instance will not be over-ridden but instead will be added as a separate record of the Competency award.
    - Competencies can only have their expiry dates extended by re-certification if they are still current at the point the new Competency is awarded. If the Competency has already expired, it will be awarded as a new instance.
  - Evidence Required – should be ticked if the competency requires evidence.
  - Evidence Verification Required – should be ticked if the evidence requires verification.
  - Expiry:
    - Does not expire – this means the competency does not expire.
    - Expire after a set period – use to set when the competency needs to be redone. If selected other ‘unit’ fields pop up.
    - Specify expiry date when awarding – this means the competency will expire as per the award date entered.
  - **E-Learning Options:** Although present on the form, the **Awardable by E-Learning** option should not be utilised when creating Employer Competencies **–** do not change the default setting of **Cannot be awarded by E-Learning**.

System Notification:

- None.

9.4. Project and Site Competencies

Function: Setting up or amending Project, Site and Zone competencies.

System / Business Rules:

- Project, Site and Zone competencies are setup or amended via a Service Desk request.

System Notification:

- None.

9.5. Project, Sites and Zones

Function: Setting up project, sites and zones.

System / Business Rules:

- Projects will only appear in (under the **Administration** tab and **Projects** shortcut) when the company has been selected as the Contractor in Charge by the Network Operator.
- Sites can only be created by the Employer Administrator of the Contractor in Charge, Advanced Project Administrators or the Project Administrator.
  - When adding a site, fields marked with a red asterisk are mandatory
- Zones can only be created by the Employer Administrator of the Contractor in Charge, Advanced Project Administrators or the Project Administrator.
  - When adding a zone, fields marked with a red asterisk are mandatory
- Setting project, site and zone competency prerequisites is completed by the Employer Administrator of the Contractor in Charge, Advanced Project Administrators or the Project Administrator.

System Notification:

- None.

10. BLOCKS AND SUSPENSIONS

10.1. Network Blocks

Function: Applying Network Blocks onto a cardholder’s profile.

System / Business Rules:

- System rules implemented are as per the RIW Blocks and Suspensions Business Rules.
- Network blocks are placed by those with full Network Operator administrator permissions and the Service Desk on behalf of the NRIWGC and/or Network Operator.

System Notification:

- When a Network Operator places a Network Block, the Primary Employer’s Employer Administrator is sent an **URGENT: cardholder number – worker name – Blocked** email, informing the employer the cardholder has no authority to work on the network whilst the block is in place.

10.2. National Blocks

Function: Applying National Blocks onto a cardholder’s profile.

System / Business Rules:

- System rules implemented are as per the RIW Blocks and Suspensions Business Rules.
- National blocks are placed by the Service Desk on behalf of the NRIWGC and automatically as a result of a failed D&A via the AHP.

System Notification:

- When a National Block is placed, the Primary Employer’s Employer Administrator is sent an **URGENT: cardholder number – worker name – Blocked** email, informing the employer the cardholder has been blocked nationally and has no authority to work on any rail network.

10.3. National and Network Job Role and Competency Suspensions

Function: Suspending a National and/or Network Job role or competency on a cardholder’s profile.

System / Business Rules:

- System rules implemented are as per the RIW Blocks and Suspensions Business Rules.
    - Network Operators can suspend or restore National Job Roles and Competencies and their Network Job Role and Competencies.

System Notification:

- No notifications are sent.

10.4. Premium Functionality Employer Job Role and Competency Suspensions

Function: Suspending a Premium Functionality Employer job role or competency on a cardholder’s profile.

System / Business Rules:

- System rules implemented are as per the RIW Blocks and Suspensions Business Rules.
  - Premium Functionality Employers can suspend or restore only their employer-based job roles and competencies.

System Notification:

- No notifications are sent.

11. CARDHOLDER EMPLOYMENT

11.1. Primary Employment

Function: Gaining primary employment.

System / Business Rules:

- To search for a cardholder, the RIW Number, Surname and Date of Birth must be known.
- Cardholders have the option to accept or reject requests for employment via their myRIW profile, which must be accepted before access to their record is allowed.

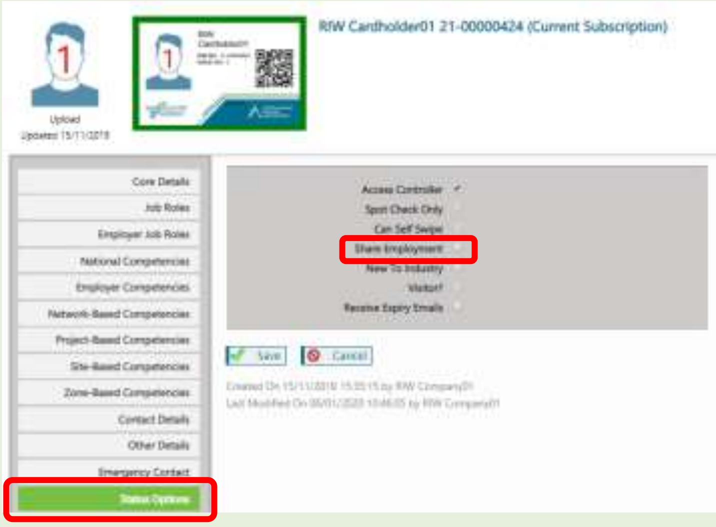
System Notification:

- An **Employment Request** email is sent to the cardholder's email address listed in the system with a link inviting them to accept the employment request from the **Employment & Associations** section on the myRIW home page.

11.2. Primary and Secondary Employment relationships

Function: The RIW System allows each cardholder to have one primary employer and up to two secondary employers.

When a primary employer creates/edits a cardholder's profile, there is the option to flag the cardholder status as active **Share Employment**, which allows the cardholder profile to be shared by a maximum of two other companies. The **Share Employment** tick box is available from the **Status Options** within the cardholder's profile as shown below. The primary employer is the only user who has the ability to alter the share employment status.



RIW Cardholder01 21-00000424 (Current Subscription)

Access Controller ✓
Spot Check Only ○
Can Self Swipe ○
Share Employment ○
New To Industry ○
Visitor? ○
Receive Expiry Emails ○

Created On 15/11/2018 15:55:15 by RIW Company01
Last Modified On 06/01/2020 10:46:05 by RIW Company01

System / Business Rules:

- The primary employer is the cardholder's direct employer and has full edit rights to the cardholder's profile.
- The secondary employer has view only rights of most aspects of the cardholder's profile, however this includes minimal edit rights as secondary employers can only assign national and network competencies to cardholders.
- To search for a cardholder to employ, the RIW Number, Surname and Date of Birth must be known.
- Cardholders who do not have the Share Employment flag set on their record cannot be employed by secondary employers.
- Cardholders have the option to accept or reject requests for shared employment via their myRIW profile, which must be accepted before access to their record is allowed.
- The primary employer is the only employer who can switch on/off a cardholder's shared employment.
- Where the cardholder has multiple employers, when the cardholder is swiped onto Site the cardholder must tell the Access Controller who they are working for on that shift.
- Any swipes that are generated by the cardholder on or after the start date (regardless of where the cardholder worked or under which employer) will be visible to all employers and associated companies.
- Shared cardholders will be available for inclusion in swipe reports for the period in which the secondary employment is valid, but not before or after.
- Premium Functionality Employers are also able to award their own employer job roles and competencies to secondary employees.

System Notification:

- An **Employment Request** email is sent to the cardholder's email address listed in the system with a link inviting them to accept the employment request from the **Employment & Associations** section on the myRIW home page.
- If the cardholder rejects the employment request, the request will be moved from the requesting employer's **Pending Approval** tab to the **Rejected** tab, where they will remain visible for 30 days.
- If the cardholder accepts the employment request, the request will be moved from the employer's **Pending Approval** tab to the **Approved** tab, where they will remain visible for 30 days.
- If a cardholder has multiple employers and the shared employment flag is then unticked, all employers except the primary employer will be removed from the cardholder's profile and an **End Employment Notification** email is sent to the Employer Administrators of the secondary employers.

11.3. Association

Function: Association is ongoing and advanced visibility of a cardholder's profile, who is not directly the company's employee.

System / Business Rules:

- To search for a cardholder to associate with, the RIW Number, Surname and Date of Birth must be entered via the **Search for New Associate** shortcut. If the cardholder appears in the list, highlighting and selecting **Associate** issues an association request.
- If the cardholder rejects the association request, the request will be moved from the requesting company's **Pending Approval** tab to the **Rejected** tab, where they will remain visible for 30 days.
- If the cardholder accepts the association request, the request will be moved from the company's **Pending Approval** tab to the **Approved** tab, where they will remain visible for 30 days.
- Association can be ended by the cardholder or the Employer Administrator.

System Notification:

- An **Association Request** email is sent to the cardholder's email address listed in the system with a link inviting them to accept the association request from the **Employment & Associations** section on the myRIW home page.
- If the cardholder rejects the association request, the request will be moved from the requesting employer's **Pending Approval** tab to the **Rejected** tab, where they will remain visible for 30 days.
- If the cardholder accepts the association request, the request will be moved from the employer's **Pending Approval** tab to the **Approved** tab, where they will remain visible for 30 days.

11.4. Ending employment of a cardholder

Function: Ending primary and secondary employment.

System / Business Rules:

- Employment is ended by an Employer Administrator entering a leave date.
- As per date section 3.2, the cardholder's employment is released at two minutes past midnight (0002/12:02am) AEST (Australian Eastern Standard Time) irrespective of the time zone in which the record/data is added.

System Notification:

- If a primary employer ends their employment, any listed secondary employer will be sent a **Primary Employment End Notification** email notifying them that the cardholder no longer has a primary employer and therefore no authority to work.

11.5. Linkage

Function: Linkage is a form of association that occurs when a RIW cardholder is swiped or spot checked and links the cardholder with the specific Network Operator or Contractor in Charge running a project.

System / Business Rules:

- If the RIW cardholder has not been associated or is listed as a secondary employer, any swipes of that RIW cardholder on or after the start date (regardless of where the cardholder worked or under which employer) will be visible to all employers and associated companies.
- When the cardholder is swiped on another Network or Project, the visibility link is broken and swipe information is now visible to the new Network and Project.

System Notification: None.

12. PREMIUM FUNCTIONALITY

Premium Functionality Employers include Network Operators and larger organisations that have access to additional functionality within the RIW System. This includes:

- Employer job roles and competencies – see section 9.2 & 9.3 for further information,
- Additional user permission of Advanced Project Administrator – see section 5.7 for further information,
- Standard Crews and Project Crews
- Allocated items management, and
- Pay on account facilities – see section 13.1.2 for further information.

12.1. Crew Differences

Function: The differences between Project Crews and Standard Crews.

System / Business Rules:

- Advanced Project Administrators can create project crews made up from primary, secondary, associated and linked cardholders. The Advanced Project Administrator must know the cardholder's surname, date of birth and RIW number to add the cardholders prior to swiping on.
- If the cardholder has swiped on they are automatically added to the project crew.
- Employer Administrators can create standard crews made up of primary, secondary and associated cardholders. These cardholders have already been added to the workforce pool by having accepted the employment / association request previously.
- Project Crew functionality will only be available if the company is a Premium Functionality Employer and the company has been selected as a contractor in charge of a project.
- After and during the life of the Project, all historical information is maintained, i.e. swipes, crew membership

System Notification: None.

12.2. Allocated Items

Function: Managing allocated items.

System / Business Rules:

- Allocated items list is a predefined list set by the Service Desk.
- Customising the list can be done via a Service Desk request.
- Cardholders can monitor their allocated items via myRIW.

System Notification: None.

13. ONLINE PAYMENT PROCESSING

13.1. Online shopping basket

Function: Employer Administrator with payment rights or Advanced Project Administrators may add or remove single or multiple items to the shopping basket, and checkout the basket. This could include ID checks, fast tracked competencies and cardholder subscriptions.

System / Business Rules:

- The Shopping Basket, and the items it contains, will be visible to Employer Administrator's, Employer Administrator – No Payment and Advanced Project Administrators.
- Only Employer Administrator's and Advanced Project Administrators have payment rights to process the shopping basket.
- The Employer Administrators – No Payment permission allows items to be added to the basket but they cannot process the payment.
- Standard employers will have access to the credit / debit card and PayPal payment options.
- Premium Functionality Employers have access to the Pay on Account payment option.

System Notifications:

- As per the transaction basket payment options listed below.

13.1.1. PayPal

Function: Paying for RIW System transactions via PayPal and Credit Card.

System / Business Rules:

- PayPal options are available to Employer Administrators with payment rights and Advanced Project Administrators.
- If paying by **Card / PayPal**, the user is moved seamlessly out of the RIW System to the online merchant PayPal platform, which securely completes the financial transaction, at which point the user is then returned to the RIW System which confirms the process is complete.
- If two payment options are present, by default, the **Card / PayPal** button is automatically selected, which grants the Employer Administrator options to:
    - Pay by a credit card stored in the employer's existing **PayPa**l account,
    - Create a new **PayPal** account, or
    - Checkout as a guest via **Card Payment** to pay by credit/debit card.

System Notifications:

- A **RIW Order Confirmation** email is sent to the Employer Administrator once the order has been processed.

13.1.2. Pay on account (POA)

Function: In addition to Credit / Debit card and PayPal options, Premium Functionality Employers have the option to Pay on Account.

System / Business Rules:

- Once a transaction is paid on account, it is actioned immediately in the RIW System and is considered technically paid. An invoice will be sent out at a later stage by the Metro Trains Australia Accounts Receivable Team to finalise payment.

System Notification:

- A **RIW Order Confirmation** email is sent to the Employer Administrator once the order has been processed.

14. AUTHORISED HEALTH PROFESSIONAL (AHP)

14.1. Recording a Medical Result

Function: Authorised Health Professional recording a medical result.

System / Business Rules:

- With the exception of Transport for NSW, the system administers the rules as per the National Standard for Health Assessment of Rail Safety Workers – https://www.ntc.gov.au/codes-and-guidelines/national-standard-health-assessment-rail-safety-workers for Category 1, 2 & 3 health assessments.
- For TfNSW, Category 3 health assessments expire every 5-years.
- Where a cardholder holds both TfNSW roles and other Network roles, the system will manage the expiries based on these rules.
- The system manages health assessment outcomes as per the following table:

Medicals held	Assessment Outcome	Outcome Selected by AHP	Result Selected by AHP	Impact on worker
Cat 1 & 2	Unfit for Cat 1	Unfit for Cat 1, but fit for Cat 2 & 3	Fit	Unfit for Cat 1. New Cat 2 recorded
		Or Cat 1	Unfit	Unfit for Cat 1. Cat 2 remains current
	Unfit for Cat 2	Cat 2	Unfit	Unfit for Cat 1 & 2
Cat 1 & 3	Unfit for Cat 1	Cat 1	Unfit	Unfit for Cat 1. Cat 3 remains current
	Unfit for Cat 3	Unfit for Cat 1, 2 and 3 but fit for work outside the dangerzone	Fit	Unfit for Cat 1, 2 & 3
		Or Cat 3	Unfit	Unfit for Cat 1 & 3
Cat 1, 2 & 3	Unfit for Cat 1	Unfit for Cat 1, but fit for Cat 2 & 3	Fit	Unfit for Cat 1. New Cat 2 fit is recorded. Cat 3 remains current
		Or Cat 1	Unfit	Unfit for Cat 1. Cat 2 & 3 remain current
	Unfit for Cat 2	Unfit for Cat 1 & 2, but fit for Cat 3	Fit	Unfit for Cat 1 & 2. New Cat 3 fit is recorded.
		Or Cat 2	Unfit	Unfit for Cat 1 & 2. Cat 3 remains current
	Unfit for Cat 3	Unfit for Cat 1, 2 and 3 but fit for work outside the dangerzone	Fit	Unfit for Cat 1, 2 & 3
Cat 2 & 3	Unfit for Cat 2	Cat 2	Unfit	Unfit Cat 2. Cat 3 remains current
	Unfit for Cat 3	Cat 3	Unfit	Unfit for Cat 2 & 3
	Unfit for Any Category	No Medical Level	Unfit	Unfit for any work

- Temporarily Unfit or Permanently Unfit may change the validity of certain competencies and/or job roles held by the cardholder.
- An AHP can only search for the cardholder by knowing the Surname, RIW Number and Date of Birth.
- All fields on the online form marked with a red asterisk are mandatory fields.
- Examination date is automatically set as the date of entry and the expiry is set based on the date of birth and category of health assessment selected. TfNSW rules are applied in the backend of the system where a Category 3 is recorded.
- Expiry dates can be brought forward by the AHP but the system prevents extending the date.
- Individual attached files are limited to 10Mb.
- The medical outcome will not be valid until the attachment is uploaded.

System Notification:

- As a result of an AHP applying an unfit status, the Employer Administrator is sent an **Unfit Medical Result** email confirming the cardholder has been deemed unfit and therefore any role requiring that medical will no longer be valid.
- **Note:** If the cardholder holds multiple medicals the email does not indicate which of the medicals changed from fit to unfit. The Employer Administrator would need to log in to the system to determine which certificate had changed state.

14.2. Recording a D&A Result

Function: Authorised Health Professional recording a D&A result.

System / Business Rules:

- An AHP can only search for the cardholder by knowing the Surname, RIW Number and Date of Birth.
- All fields on the online form marked with a red asterisk are mandatory fields.
- Examination date is automatically set and the expiry set based on the date of birth.
- Individual attached files are limited to 10Mb.
- The D&A outcome will not be valid until the attachment is uploaded
- Any failed D&A result recorded via an AHP results in a National Block. This block is a sum of individual network blocks which enables those Network Operators with a second chance/rehabilitation program to lift the block on their network with the block still remaining on the other networks.

System Notification:

- If the outcome from a D&A screen was a fail, the Employer Administrator is sent a **D&A Test Positive Fail** email confirming the cardholder has been deemed unfit and therefore any role requiring that medical will no longer be valid.
- **Note:** D&A tests conducted via random, post incident or show cause are administered via the blocks and suspensions process and not via the AHP user permission.

15. REGISTERED TRAINING ORGANISATION (RTO)

Function: A registered training organisation uploading a competency into a cardholder's profile.

System / Business Rules:

- RTO awardable competencies are setup by the Service Desk via a service request (https://www.riw.net.au/contact-us/request-a-service/).
- A RTO can only request setup of competencies they are permitted to award. (National, Network or Employer)
- Requests for assignment of Employer based competencies must be made to the Employer who owns the competency.
- To search for a cardholder to award a competency individually or to multiple cardholders, the RIW Number, Surname and Date of Birth must be known.
- If a competency has been suspended by the Network Operator and was configured as **Update Existing Award**, then the competency can be re-uploaded by the RTO, but remains invalid.
- If a competency has been suspended by the Network Operator and was configured as **Always Award as New**, then the competency can be re-uploaded by the RTO, but remains invalid.
- Competency files must be either PDF, JPG or PNG of less than 10Mb in size.

System Notification:

- None.

16. KINEO

Function: Automated emails associated with e-learning.

System / Business Rules:

- All competencies must be setup via a service request to the Service Desk. As part of this, e-learning can be chosen as the preferred delivery method.

System Notification:

- The following system emails are generated and for what reason:
  - **RIW E-learning Course Completion requested (payment required)** – This email is sent to the cardholder indicating they are required to pay and complete the specified course. A hyperlink is provided in the email.
  - **E-learning Course Completion requested** – This email is sent to the cardholder indicating they are required to complete the specified course. A hyperlink is provided in the email.
  - **Password Reset** – this email is sent to the cardholder allowing them to reset their Kineo password when the user clicks on ‘Forgotten your username or password’ on the eLearning login page.

17. GLOSSARY

The RIW System & Program Glossary is available on the RIW Knowledge Centre here.

18. APPENDIX 1 – USER PERMISSIONS

The RIW System User Permission Matrix is available on the RIW Knowledge Centre here.