Australian Government
Australian Financial Security Authority

RESPONSIBLE PPSR REGISTRATION MANAGEMENT

PPSR
Personal Property Securities Register

Principles for managing **PPSR registrations to support data integrity**

ppsr.gov.au

The Australian Financial Security Authority (AFSA) administers the Personal Property Securities Register (PPSR) and would like to see as many people understand and benefit from the PPSR as possible. Supporting better outcomes for consumers, business and the community.

CONTENTS

WHY CREATE THESE GUIDELINES?

The Personal Property Securities Register (PPSR) is an important financial tool in Australia that helps to support our economy. As an online noticeboard, we all want it to be accurate and up to date.

> Data integrity is key to having a reliable register, and having a reliable register promotes confidence in its use.

The PPSR operates best when everyone using it has a shared understanding about how best to manage data that is held on it.

This guide sets out principles to promote the responsible management of PPSR registrations, including tips and real-life examples.

For PPSR registrations, a shared understanding includes knowledge of:

- what can be registered
- how registrations are created and maintained
- how to remove expired registrations
- how to identify, remove or correct registrations that contain errors or are ineffective.

Without a shared understanding, there is a risk that:

- registrations may be incorrect
- expired registrations might clutter up the register and make searches less effective
- malicious interference with registrations might occur
- the integrity of the register ***might not be maintained***.

WHO ARE THESE GUIDELINES FOR?

These guidelines are for anyone registering a security interest on the PPSR. This includes those who provide registration services to others, as well as those users making their own registrations.

If you offer services that help people to make a PPSR registration, it is ***very important you understand the scope of the promises you are making*** and are able to demonstrate that the people in your business have the appropriate skills, qualifications or experience to make those promises. You must be appropriately insured and deliver your services competently and in compliance with all laws.

A business providing an administrative service to assist in completing a registration will be different from a service that tells clients that their interests will be protected.

If you tell clients their interests will be protected, regardless of any disclaimers, the expectation of the client will be that you have the necessary qualifications and experience to provide that advice.

IMPORTANT NOTE:

These are guidelines only. Meeting these guidelines does not replace, or guarantee that you are compliant with, your obligations under the *Personal Property Securities Act 2009* or the regulations. You remain responsible for your compliance.

STEPS TO RESPONSIBLE MANAGEMENT

What can you do?

When we talk about responsible management of registrations, we encourage proactive management and consideration of these key areas.

Responsible registration management recognises the vital role users play. This guide aims to help users act responsibly, share learnings with users, and highlight some of the areas we believe users should focus on. Should it be registered? It is important to know which agreements should be registered, as not everything belongs on the PPSR.

Accuracy

The consequences of inaccuracy depend on the type of error. At worst, the registration may be entirely ineffective.

Currency

A lapse in the currency of a registration can have serious consequences for priority and in insolvency, effectiveness.

Timely

For registrations to provide certain rights, timing is crucial.

Security controls

Actively managing the security helps protect against misuse.

Monitoring

Do you know what your staff and customers are doing?

BEFORE YOU REGISTER

An effective registration on the PPSR helps to protect the financial interests of a business.

Before you begin the process of registering a security interest on the PPSR, there are some important things to consider:

- What can/should be registered?
- What shouldn't be registered?
- Storing supporting evidence
- What happens when a registration is made without a valid security interest?

What can/should be registered on the PPSR?

The PPSR is a noticeboard notifying an interested party that there is a security interest over property.

This could, for example, be in connection with a seller awaiting payment under a retention of title agreement, or a lender who provided the money to purchase particular goods or assets.

The security interest is fundamental. Without a security interest, a registration will be invalid. It is important to consider whether there is, or will be, a valid security interest prior to making a registration

What should not be registered on the PPSR?

The PPSR is a noticeboard of security interests – ***it is not a record of ownership***.

Here are some things we have seen that are examples of registrations that are not acceptable:

- registering an interest without having a valid security interest (or expecting to have one)
- making vexatious registrations
- using the register with the intention of holding up or otherwise interfering with a transaction
- making duplicate registrations for no proper purpose
- making registrations on the live PPSR that are for testing purposes – we have a testing environment known as Discovery.

Storing supporting evidence

When creating a registration, you will need to use the details of the agreement giving rise to the security interest. Importantly, the PPSR is a noticeboard only – the actual documents or evidence supporting the security are not stored on the PPSR.

The secured party should have some form of written proof of the transaction, whether by formal legal agreement or otherwise.

It is important this evidence is kept safe, as it may be necessary to produce it in the future to prove a claim, or to meet statutory obligations to provide information as the secured party.

Some providers elect to collect this information and retain it on behalf of their customer, while others leave that responsibility with their client. In either circumstance, you should consider what would be required to prove the security interest seven years after the date of registration if the grantor became insolvent.

Neither you nor your clients want to be trawling through email archives to prove a transaction when priority of security interests, and possible recovery, is at stake.

What happens when a registration is made without a valid security interest?

You must not apply for registration of a financing statement unless you have reasonable grounds to believe you are (or will be) a secured party in relation to the collateral.

There are consequences for the intentional or unintentional misuse of the PPSR.

Consequences may include civil penalties and a damages claim if the misuse causes harm to another party.

ACCURACY OF INFORMATION

As a noticeboard, the PPSR is only effective if the information stored on it is accurate.

There are some simple principles you can use to help support data integrity:

- Use validation tools to improve data accuracy.
- Get the grantor right.
- Properly use the Giving of Notice Identifier (GONI) field.
- Only make multiple registrations when it's okay.
- Review the data on your verification statement.

Importance of accurate data entry when creating a registration

The PPSR is the online tool used to create and manage registrations, which can only be as effective as the information entered on the register.

If data, like a serial number or grantor identifier, is entered incorrectly, it can mean the registration created is not effective and may be unable to be enforced.

Validation tools

The PPSR has inbuilt functionality to support quality data when creating and managing registrations, including validation, review and verification services.

> If you are a business-to-government (B2G) user or provide a registration service to the public, you can build in additional checks, prior to submitting your request to the PPSR.
> These checks can be manual or built in to your user interface.

Remember, you are responsible for the system you build. If you get it wrong, you may be held responsible. This might include things like incorrect registrations that cause a secured party to lose their priority or additional fee payments for ineffective registrations.

Additional validation tools and processes that we have seen implemented include:

- **Double-blind entry.** Using double-blind entry for important identifiers such as ACNs or serial numbers.
- **Smart templates.** Creating smart templates to provide additional information and to ask additional questions.
- **Secondary Checks.** Having a second person, or software, that checks and verifies a draft instruction before it is submitted to the PPSR, particularly with higher value collateral.
- **Help wizards.** Wizards to help users choose registration details such as collateral.
- **Prefilling information.** Prefilling information from other systems to reduce copying errors.

IMPORTANT NOTE:

We are only providing you with guidelines and some examples, which may not be suitable for all circumstances. If you have any doubts about the accuracy of your system or the recommendations you make for your customers, you should engage a professional adviser, such as a lawyer, to review your system.

Get the grantor right

For people making a registration directly through the PPSR, there is a process to help choose the right grantor and verify details like ACNs and ABNs, but that still doesn't guarantee that a grantor has been properly identified.

Where a grantor has been incorrectly identified in a registration, the registration will be ineffective, leaving you unprotected.

If the error is not discovered, the registration may stay on the PPSR, misrepresenting the named grantor's business and potentially causing them detriment.

You could be liable to both the secured party for their loss of security and the misrepresented grantor if they suffer harm.

There may be instances during the course of an agreement where the grantor may need to change. It is important that you, or your clients, understand the agreement well enough to identify these instances. An example might be where the collateral changes hands, or when the grantor identifier changes.

How to use the GONI field

The Giving of Notice Identifier (GONI) is a field where you can enter text to help identify the registration. Essentially, it is your internal reference number.

This GONI is available to the public when they search the PPSR and is useful in identifying an individual registration, particularly if you have many registrations with similar secured party, grantor and collateral details. A person serving a notice on the secured party has an obligation to include the GONI in their notice.

B2G TIP

If the GONI is key to internal identification of a registration, consider making this field mandatory in your user interface.

Check the verification statement

The verification statement is a confirmation of the registration created and should be reviewed as soon as you receive it.

If you notice an error in the verification statement, you should amend it immediately, because some errors will make your registration ineffective. Note that not all fields on a registration can be amended – you may need to create a new registration. For more information see ppsr.gov.au.

When are multiple registrations of the same security interest okay?

A registration is made over a single collateral class, which means you may have to make multiple registrations for a single security agreement, and that's okay.

Where there are different interests in the same collateral – for example, a purchase money security interest (PMSI) and a non-PMSI, then it may be appropriate to register both of those interests to protect the potential for priority of the PMSI.

It may also be administratively convenient if secured obligations are being transferred to another party or to create overlapping registrations as one nears its end date. The PPSR is not set up to check for duplicate entries of the same data or raise alerts in the registration process to let you know that the same registration already exists.

Getting a registration right is important, and we are aware of circumstances where people make multiple registrations to cover off all options 'just in case'. This is not recommended, as it creates clutter on the register.

TIP

If you are unsure how to accurately register a specific security interest, it may be worth seeking legal advice. There may be examples where legal advice is unclear about how a registration should be made and the risk of an error is managed by registering 'both ways'. However, this should not occur as a matter of course. If there is a clear means of making an effective registration, then ancillary registrations should not be made.

CURRENCY OF INFORMATION

As the PPSR is a real-time noticeboard of security interests, available to users 24/7, making sure the information is current and up to date is essential for effective searching. Some considerations to help with currency include:

- reviewing registrations with no stated end date – they have the potential to become clutter
- extending a registration before it expires
- keeping your address for service up to date
- building in systems and controls to manage key points of the registration life cycle – amendment and discharge.

Extending an expiring registration

If a secured party has a registration which is due to end, and the money owed is not expected to be repaid before the expiry date, then the secured party may wish to amend the registration to extend the end date.

As long as there is a continuing security interest, the secured party may extend the expiry date of a registration. The amendment to the end date must be completed before the expiry date to maintain the original priority date of the registration.

Without keeping track of expiring registrations, a secured party is at risk of losing priority of their interest.

TIP

You cannot extend a registration once it has expired. Run the 'registrations due to expire' report to keep on top of your expiring registrations. The Registrar is unable to restore expired registrations for you.

Reviewing registrations with no stated end date

A registration which does not have an end date runs the risk of not being updated if the circumstances change, unless there are checks in place to ensure it remains current.

'No stated end date' registrations should be discharged in a timely manner. When the obligation has been satisfied, the secured party is responsible for discharging the registration promptly.

TIP

Create a process to ensure 'no stated end date' registrations are regularly reviewed for relevancy and promptly discharged or amended as required.

Keeping your details up to date

The address for service for your secured party group is very important. It must always be kept up to date.

Why is this so important?

The address of the secured party on a registration must be kept up to date as it is the address used:

- by the Registrar of Personal Property Securities to communicate about registrations (e.g. to deliver an amendment notice)
- by any party who needs to query the registration.

If an address for service of a secured party is not kept up to date and the Registrar attempts to contact the secured party with an amendment notice, failure to respond could result in the removal or discharge of that registration.

The PPSR facilitates keeping details up to date through its secured party group functionality. An update to the details of a group is reflected in all registrations connected to that group.

B2G TIP

Educate your customers about keeping their information up to date and why it is important. Build into your system a process to make sure updated customer information you receive is promptly updated on the PPSR.

Build in systems and controls to manage key points of the registration life cycle – amendment and discharge

Checking the verification statement is an important step to ensuring your registrations are accurate; however, as agreements change over time, so should the registration.

If you provide PPSR support services, it is important to educate your customers – make sure they understand that they need to let you know if a registration is no longer required (for example, if they have a loan paid out early). This will enable you to promptly discharge registrations where the security interest has been satisfied.

Think about building into your system the ability to monitor and update your registrations.

What might this look like? Here are some pointers:

- When an agreement is amended, are you alerted to check the registration details?
- When a loan is finalised, is there a trigger to discharge the registration?
- As registrations approach expiry, what process will alert users to review and extend if needed?

TIMELINESS

For registrations to provide certain rights, timing is crucial.

Some considerations around timing include:

- Why is timing important?
- Registering before the deal is done is a great idea, but make sure the registration is discharged if the deal does not proceed!
- Discharge in a timely manner.

Why is timing important?

As the PPSR works on priority, you should register as soon as possible to give yourself the best possible chance of protection.

While it is prudent to register an interest as early as possible, there are also statutory timelines you must be aware of.

For example:

- **The Personal Property Securities Act 2009**
  The Act sets out requirements for registration timing in relation to purchase money security interests (PMSI). For more information on PMSI, see ppsr.gov.au
- **The Corporations Act 2001**
  The Act sets out requirements for registration timing against company grantors to protect you against their insolvency.

Failure to comply with these timing requirements can have significant consequences, so it is important that you understand when these apply.

Registering before the deal is done?

Registering a security interest prior to the deal being finalised is an acceptable use of the PPSR.

To register in this manner, you must have a genuine belief that you will have a security interest, and you must make sure the registration is promptly discharged if the deal falls through.

Example: A financier has approved a car loan for a customer who is due to collect the car from the dealer the following week. The financier registers a security interest in anticipation of the customer collecting the car.

This is important for the financier as they need to make sure their interest is protected before the customer takes possession of the car – this is an acceptable use of the PPSR.

The customer has a change of heart and decides not to go ahead with the car purchase. The financier no longer has a security interest in the car and must promptly discharge their PPSR registration.

Discharging in a timely manner

Secured parties should discharge registrations in a timely manner, but some registrations have legislated timeframes.

For example, if your registration is for serial-numbered goods (such as a car), or consumer collateral, you must discharge the registration within 5 business days of repayment.

We are aware of cases where searches conducted as part of a sale-of-business process reveal registrations that should have been removed from the PPSR months or even years earlier. Where those searches are completed on the day of settlement, it is not always possible to have them discharged the same day, which can delay the transaction.

TIP

It is a good idea to create a process to ensure a registration is promptly discharged on repayment of a loan, even if the loan is repaid early.

SECURITY CONTROLS

Protecting data is not just about passwords– although passwords are important.

The Australian Cyber Security Centre leads the Australian Government's efforts to improve cyber security. As this is a specialised field, we won't provide detailed recommendations, but there are some principles specific to the PPSR that you should consider:

- risk strategy
- personnel security
- passwords, tokens and access codes
- using system permissions to restrict access
- keeping software and systems up to date
- backing up your data.

For more information about cyber security, see **cyber.gov.au**.

Risk strategy

The commercially sensitive nature of information required for registrations on the PPSR puts businesses using the PPSR and storing client information at risk of cyber security threats.

Security planning in your operating system, secure data storage and security-mindful business processes should be part of your risk strategy.

Imagine if:

- someone without authorisation accessed your system and amended or discharged your registrations
- you had a data theft and the stolen data was used to amend or discharge other parties' registrations
- the client information you hold was stolen and sold as a customer list
- someone in your business used your access to create registrations that amounted to criminal behaviour.

The Australian Cyber Security Centre has a range of resources available for individuals and businesses.

Go to cyber.gov.au for resources.

Consider personnel security

As a service provider, it is your obligation to ensure your personnel have at least a basic understanding of cyber security, including the risk of data loss, destruction or theft.

It is also your obligation to have protocols in place to reduce those risks and to make sure the protocols are followed.

As a first step, your business should have a clear understanding of who can use your PPSR account and the extent or limits on their access.

Some questions you should consider:

- Do you conduct police and pre-employment checks on personnel who will have access to data?
- Is it appropriate that everyone on staff has access to your system login, or should access be restricted to identified users?
- Is access available only from your premises, or anywhere, anytime on mobile devices?
- Should users have access to the full life cycle of a registration, or do you limit users to access for monitoring and reporting only, or creation only, or deregistration only?
- Do you know who in your business has the responsibility to oversee and monitor use of your access to the PPSR?
- Do you have protocols in place for removing access for people who have left your business or changed divisions?
- Do you limit access to stored information?
- Do you monitor access to stored information?

Know your customer

As a business-to-government (B2G) provider, you are responsible for the transactions performed through your B2G account.

Even though you might be transacting on behalf of a third-party user, our contractual arrangement is with you as the PPSR account owner. So it is important to know who your customers are and the transactions they are performing via your service.

Passwords, tokens and access codes

Users should understand the importance of not sharing usernames, and protecting passwords, but also need to understand that secured party group (SPG) access codes and registration tokens are just as important.

If someone has access to an SPG number and access code, they can amend or discharge any registration within that SPG.

Everyone in your business who has access to use your PPSR account, or clients who have access, should comply with security practices such as:

- protection of usernames and passwords
- prohibition on sharing username and/or password information
- protection of SPG codes and registration tokens.

You should also ensure staff regularly receive security training.

Restrict access

To limit the impact of a cyber security incident, it is important to consider when it is best to restrict access.

Users should only be given access to applications based on their duties. It is important to manage this and remove access when a user's role changes, or when they are no longer employed.

Some businesses implement further restrictions through multi-factor authentication for staff, or require administrator accounts to gain access through the use of virtual private networks or remote connections. You should consider appropriate steps for your business.

Consider restricting permissions for those who have access. You can imagine the impact if someone discharged your registrations by mistake or intentionally. The impacts on your business could be severe and costly. Restricting permissions can help to limit damage – see the 'System permissions' subsection on page 26 for more information about how to restrict PPSR permissions.

TIP

Whatever strategies you have in place, audits and regular access and permission reviews are an easy step to help prevent possible incidents.

System permissions

The PPSR allows the system administrator to provide permissions as required.

- Financial transactions such as payments can have restricted access
- Who should have access to create, amend and discharge registrations?
- Apply the doctrine of least access – only provide access when it is required to perform a function
- Where possible, segregate user access roles – this is particularly important where there are users and developers working in the same organisation

The PPSR has a 'permission-based' control method, which is available to account users.

This model allows you to assign a permission level to each task, which will let you limit access to certain tasks. You can set permissions for actions like:

- creating registrations
- discharging registrations
- making payments
- managing SPGs.

Using these permission levels, account administrators can create customised permission sets (groups) for each user type in their organisation. This is an effective way to ensure each user within your organisation can only use the PPSR functions relevant to their job.

TIP

Set a higher level of security for groups with higher risk permissions – for example, groups that can make discharges. A discharge cannot be undone, and a customer may lose their priority if their registration is discharged in error.

Keeping your software and systems up to date

It is a surprise to some people that a failure to keep software up to date creates security risks.

Most hardware now comes preloaded with software, and software must be regularly updated, in part to apply security updates against emerging threats.

A failure to keep systems current could mean a business is operating with outdated software, which can be a security threat. This also applies to the browser you are using and whether it is up to date.

If you are using the PPSR via our web interface, you should ensure that the web browser you are using to access ppsr.gov.au is the latest version.

All B2G users should also make sure the data they are sending to the PPSR uses the highest security measures, like strong cyphers and newer TLS versions.

Back up your data

> Backups are like insurance – we hope we never have to use them, but it is important to have them there … just in case!

Should you be unlucky enough to experience a security incident, it will be important to have a backup of your data so that you can restore it.

Make sure backups are done regularly and that you can actually retrieve and use data from your backup system. Consider additional security measures for your backup, such as encryption. Offsite backups and remote backups are good practice, ensuring your backup is not permanently connected to your main operating system or connected by a local network.

MONITORING

Maintaining the accuracy and currency of information on the PPSR must be supported by good monitoring practices. Do you know what your staff or customers are doing?

Some key principles to consider include:

- Look for unusual activity
- Monitor system permissions – especially those with higher levels of access
- PPSR reports to monitor activity
- System alerts
- Make your customers and staff aware of the audits and monitoring

Looking for unusual activity

It is common practice for technology departments within businesses to have levels of monitoring over their hardware and software.

The monitoring looks for, among other things, uncommon or unusual use and can be an important tool for detecting irregular or unauthorised activities.

Examples of irregular behaviour could include a secured party sending through a request that discharges all of their registrations, or requests to perform the same transaction over and over.

The Registrar is aware, for example, of an organisation performing bulk registrations on behalf of a third party. An error crept into the registration process due to the spreadsheet being used for the registrations. In the spreadsheet, there was a column for the SPG number and the correct SPG number was entered. Unfortunately, coding within the spreadsheet caused this SPG number to then increase by one for each row in the spreadsheet. Had there not been checks in place, these registrations would have all been made in error, creating clutter on the PPSR, costing money in incorrect registrations, and wasting a considerable amount of time.

TIP

If you are performing transactions on behalf of third parties, consider monitoring processes that allow you to pick up unusual activity, such as a secured party discharging all of their registrations. These processes can be manual or automated in your system.

Monitor system permissions

As discussed in the 'Security controls' section on page 22, the PPSR allows the system administrator to assign permission as required. Limiting access to PPSR functions is an effective way to ensure each user within your organisation can only use the parts of the PPSR that are relevant to their job, but this access still needs to be monitored.

Reporting functions allow you to monitor your users to ensure they are only performing the transactions relevant to their role.

TIP

If you have staff who can perform transactions that may be high value or high risk, you should establish monitoring practices to ensure the correct people have access and are performing transactions you expect.

System alerts

There are a number of different ways that system alerts can be implemented. We recommend you consider:

- ***System alerts for errors.***
  For example, you could build intelligent systems looking for registration activities out of the ordinary and have an alert to an officer within your organisation for investigation. This might help to pick up errors in registrations.
- ***System alerts for security.***
  For example, you could build into your system an alert function that lets a designated officer within your organisation know that an unauthorised person has accessed (or attempted to access) information or registrations that are not relevant to their role. Mostly, this will probably be by innocent error; however, fraud or intentional misuse generally starts small as boundaries of your security are tested. Having clear boundaries and alerts that allow for timely investigation may assist in keeping your system secure.

PPSR reporting

The PPSR offers a number of reports that can be generated using the web interface to assist monitoring activity on the PPSR. Some examples of reports that can be helpful to monitor PPSR activity include:

- ***Account registration activity report.***
  This report allows you to view all registration transactions completed using your account. It will provide transactions completed by each user. You should monitor the information in this report and regularly conduct audits.
- ***User management report.***
  This report details all users of your account and their status, e.g. removed, deactivated, active. It can help you manage which users have access to the PPSR on your behalf and the permissions they hold.
- ***Registrations due to expire.***
  This report allows you to identify registrations that are due to expire within a specific period, providing valuable information to assist reviews and extend registrations where required.
- ***Search activity report.***
  This report provides you details of all of the searches your users have performed. This report can be used to identify those searches which should only be performed by users who have an authorised purpose, such as Individual Grantor searches.

For more information about reports that the PPSR can provide, see ppsr.gov.au/reports.

Promote awareness of monitoring

Make your customers and staff aware of audits and monitoring. Awareness of monitoring influences behaviour.

Acknowledgements

The Australian Financial Security Authority (AFSA) acknowledges and thanks industry and government stakeholders that helped formulate this Responsible PPSR Registration Management guide.

For more information visit
ppsr.gov.au