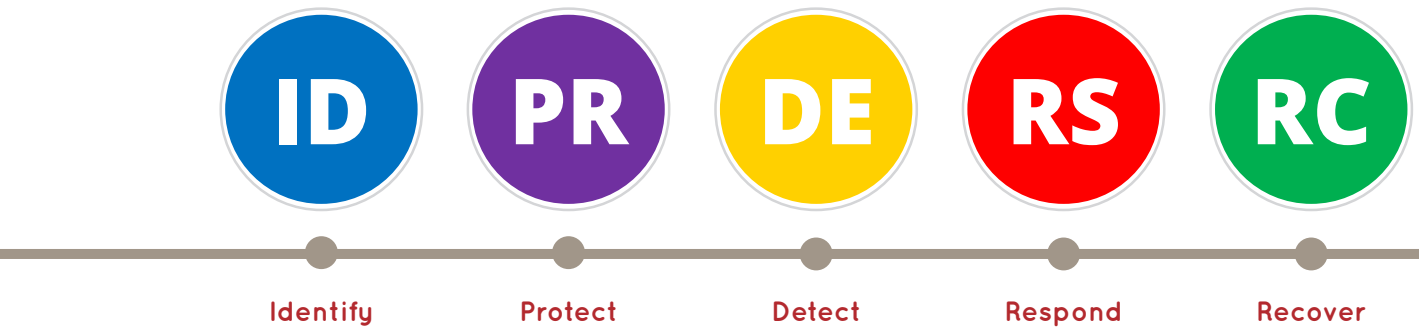
centreRED IT is committed to providing our partners with industry recognised cyber security best practices. Previously, centreRED has used the Australian Signals Directorate's 'Essential Eight' mitigation strategies as a baseline to guide our cyber security best practice. In an ever-evolving and dynamic cyber security environment, we have reviewed our Security Framework and as such, centreRED will now be guided by both the Australian Cyber Security Centre's (ACSC) 'Managed Service Provider Better Practice Principles', and the American National Institute of Standards and Technology's (NIST) 'Framework for Improving Critical Infrastructure cyber security' to complement the ASD's Essential Eight.

The Managed Service Provider (MSP) Better Practice Principles is a list of principles that specifies the list of requirements for an MSP to join the ACSC's Managed Service Provider Partner Program. Whilst centreRED is not currently active in this program, as a business we will commit to following these principles.

The NIST's Framework for Improving Critical Infrastructure cyber security provides a common language for understanding, managing and expressing cyber security risk. The Framework Core provides a set of activities to achieve specific cyber security outcomes and reference examples of guidance to achieve these outcomes. Functions within the Framework Core organise basic cyber security activities at their highest level. Those functions are:



centreRED has combined the Essential Eight mitigation strategies, the MSP Better Practice Principles and the above Functions of the NIST Framework into an easy to follow cyber security checklist. This checklist will allow us to work with our partners to form an organisational culture that addresses the dynamic cyber security risk and become proactive in implementing essential cyber security practices.

centreRED IT

14 ways to help protect your business from a Cyber Security Incident

ID

Security Assessment

It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?

Date ____ / ____ / ____

PR

Passwords

Apply security policies on your network. Examples: Deny or limit USB file storage access, enable enhanced password policies, set user screen timeouts, and limit user access.

PR

Computer Updates

Keep Microsoft, Adobe, and Java products updated for better security. We provide a "critical update" service via automation to protect your computers from the latest known attacks.

PR

Spam Email

Secure your email. Most attacks originate in your email. We'll help you choose a service designed to reduce spam and your exposure to attacks on your staff via email.

Did you know?

1 in 5 Small businesses will suffer a cyber breach this year.

81% Of all breaches happen to small and medium sized businesses.

97% Of breaches could have been prevented with today's technology.

PR

Firewall

Protect your network. A robust and intelligent firewall is the essential device allowing you to secure your network and everything that falls behind it.

PR

Security Awareness

Train your users - often! Teach them about data security, email attacks, and your policies and procedures. We offer a web-based training solution and "done for you" security policies.

PR

Multi-Factor Authentication

Utilise Multi-Factor Authentication whenever you can, including on your network, banking websites, and even social media. It adds an additional layer of protection to ensure that even if your password does get stolen, your data stays protected.

PR

Encryption

Whenever possible, the goal is to encrypt files at rest, in motion (think email) and especially on mobile devices.

PR

Web Gateway Security

Internet security is a race against time. Cloud-based security detects web and email threats as they emerge on the internet, and blocks them on your network within seconds – before they reach the user.

PR

Identity Management

Protect your identity, reduce the risk associate with password sprawl and poor password practices, and increase the speed at which a compromised user account can be shut down.

DE

Vulnerability Testing

Understanding the flaws that exist in your network and applications allows you to mitigate the critical vulnerabilities and protect your business from future cyber attacks

DE

Dark Web Research

Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach. We scan the Dark Web and take action to protect your business from stolen credentials that have been posted for sale.

DE RS

Advanced Endpoint Detection & Response

Protect your computers and data from malware, viruses, and cyber attacks with advanced endpoint security. Today's latest technology protects against file-less and script- based threats and can even rollback a ransomware attack.

RC

Backup

Backup local. Backup to the cloud. Have an offine backup for each month of the year. Test your backups often. And if you aren't convinced your backups are working properly, call us ASAP.