

# User Application Hardening Checklist

## 1. Identify and Review Applications

- ☐ Create a list of all applications installed on employee devices and servers.
- ☐ Confirm which applications are actively used in daily operations.
- ☐ Flag outdated, redundant, or unknown applications.

## 2. Remove Unnecessary Applications

- ☐ Uninstall unused or legacy applications.
- ☐ Remove trial, demo, and pre-installed software not used for business functions.
- ☐ Block employees from installing unapproved applications.


## 3. Disable Risky Features

- ☐ Disable Flash, Java, and macros unless essential.
- ☐ Turn off unused browser plugins and extensions.
- ☐ Configure applications to restrict user ability to re-enable these features.

## 4. Secure Configuration Settings

- ☐ Enable automatic updates on all applications.
- ☐ Set strong default privacy/security settings in each app.
- ☐ Restrict access to application configuration settings for standard users.

## 5. Harden Web Browsers

- ☐ Disable unnecessary browser extensions.
  - ☐ Use a secure default search engine (e.g. DuckDuckGo or Bing SafeSearch).
  - ☐ Centrally manage browser security settings via group policy.
  - ☐ Enable Attack Surface Reduction (ASR) rules where supported.
- 
- A decorative graphic in the bottom right corner consisting of overlapping blue and light blue curved shapes, resembling a stylized wave or a modern design element.

## 6. Harden Email Clients

- ☐ Disable automatic image and attachment previews.
- ☐ Warn users about emails from external sources.
- ☐ Enable anti-phishing and anti-malware protection.

## 7. Harden Microsoft Office (or Alternatives)

- ☐ Disable all macros by default (except signed/trusted ones).
- ☐ Enable Protected View for files from the internet.
- ☐ Block Office from creating child processes and injecting code.
- ☐ Disable OLE package activation.

## 8. Harden PDF Readers

- ☐ Disable JavaScript within PDF reader applications.
- ☐ Enable automatic updates.
- ☐ Restrict internet access from within PDFs if possible.

## 9. PowerShell Security

- ☐ Disable or uninstall PowerShell 2.0.
- ☐ Enforce Constrained Language Mode for users.
- ☐ Enable logging and monitoring of all PowerShell usage.

## 10. Train Your Team

- ☐ Educate staff on recognising suspicious app behaviours.
- ☐ Conduct regular reminders on safe application usage.
- ☐ Share this checklist and make security part of onboarding.

## 11. Maintain & Monitor

- ☐ Schedule a quarterly review of all application configurations.
- ☐ Monitor logs and alerts for unusual application activity.
- ☐ Test hardening effectiveness annually or after major changes.

## Need Help?

If you're unsure how to apply these changes or need technical assistance, reach out to [Netcomp](#) IT & Cyber Security. We support small businesses across Brisbane and the Gold Coast with tailored, practical cybersecurity solutions.