ALLEGR

Software Development Security Policy

Updated: 3rd December 2025

Purpose

This policy outlines our approach to integrating security at every stage of our software development process. It is based on the UK Government and MOD's Secure by Design (SbD) principles and adapted to suit our small, agile team.

Our aim is to ensure security is embedded from the outset, not treated as a final checklist or compliance hurdle. This policy provides clear principles and actionable steps to support a consistent, risk-aware approach to secure development.

Our Security Principles

We adopt the following principles across our development and delivery lifecycle:

- **Security is proactive:** It starts at the idea stage and continues through the lifecycle of the product or feature.
- **Everyone is responsible:** Security is a shared responsibility across product, engineering, and operations - not siloed to one individual or team.
- **Proportionate, not perfect:** Security controls are scaled to the criticality and complexity of the system or feature being developed.
- **Assurance is continuous:** Risk is not "signed off" at go-live. We build, test, monitor, and adapt as systems evolve.
- **User safety matters:** We design systems that protect end-users - including their data, privacy, and interactions with others.

Checklist System Overview

To ensure our Secure by Design practices are applied consistently, we use a set of internal checklists to guide and document security considerations at key points in our development process. These checklists are accessed via our website (private) and completed as online forms.

Each submission is:

- Automatically converted to a PDF record
- Stored in our internal archive for audit purposes
- Attributed to the person submitting the form, with a timestamp

This approach provides traceability, accountability, and ongoing visibility into our secure development practices.

The three core checklists are described below and accessed here:
https://www.militaryapp.org/policies/software-checklist

1. New Feature Design Checklist

This checklist is completed before development begins on any new feature.

It ensures the team considers:

- What data the feature will handle
- Potential risks from misuse or breach
- Whether new APIs or external access points are introduced
- Whether any new roles or permissions are needed
- Whether the feature allows user-generated content or interaction
- Whether least-privilege access has been applied in both code and infrastructure

2. Release Readiness Checklist

Completed before deploying a feature to staging, beta, or production environments.

This checklist covers:

- Securing all communications (internal and external) with HTTPS/SSL
- Removal of hardcoded secrets or test credentials
- Input validation and sanitisation to prevent common attacks
- Enforcement of permissions on the server side (not just UI)
- Logging of key events for audit and monitoring
- Sensible default permissions for new users or roles
- T&Cs or consent requirements (if user-facing)
- A basic peer or automated security review

3. Quarterly Security Review Checklist

Conducted every three months as part of our continuous assurance process.

It includes:

- Reviewing and updating user permissions and admin roles
- Auditing use of third-party services, APIs, or integrations
- Reviewing data storage and encryption standards
- Assessing the adequacy of moderation tools and abuse handling
- Verifying our incident response plan and escalation process
- Ensuring T&Cs, privacy notices, and consent flows remain accurate
- Reviewing the effectiveness of our SbD checklists and refining them as needed

Review and Updates

This policy will be reviewed and updated on a biannual basis or after any significant change to our development processes, threat landscape, or MOD/security requirements.

For questions or feedback, please contact the Ben Burch ben@allegr.org