

# OWASP Security Champions Guide

Principle – 1: Be Passionate About Security

Artefact: Checklist

This checklist can be used during the security champion lifecycle to ignite the passion for security in every stage.

## Attraction/Recruitment

- Hiring new employees:
  - Highlight your security culture and security champions program to attract the right people.
- Recruiting Security Champions internally:
  - Organize open sessions to get exposure for the security programs. Sessions with a small reward (like lunch sessions and pizza evenings) can trigger people to show up and learn more about the program.
  - Review their security background (if any) and discuss options for development and growth in this area.
  - Ask about the challenges and opportunities they see in their team(s), preferably with real examples.

## Onboarding

- Program introduction:
  - Explain the purpose and objectives of the Security Champions Program. Highlight the importance of their role as security advocates and influencers within the organization.
  - Emphasize how their participation will contribute to improving the overall security posture.
- Program overview:
  - Provide an overview of the program structure, including the roles and responsibilities of security champions.
  - Explain the expected time commitment and the duration of their involvement.
  - Highlight the personal benefits of the program.
  - Share success stories or case studies from previous security champions to showcase the program's impact.

# OWASP Security Champions Guide

Principle – 1: Be Passionate About Security

Artefact: Checklist

## Development/Retention

- Training and Education:
  - Provide access to relevant security training materials, resources, and documentation.
  - Arrange security training sessions or workshops to enhance their understanding of security concepts, best practices, and emerging threats.
  - Promote platforms that provide hands-on training. Gamify by organizing capture the flag events or setting up leaderboards.
  - Encourage them to pursue security certifications or external training opportunities and provide support as needed.
- Security Awareness:
  - Share information about the current security landscape, recent security incidents, and industry trends.
  - Highlight the importance of security awareness among technical staff and their role in promoting a security-conscious culture.
- Collaborative Initiatives:
  - Introduce ongoing security projects or initiatives they can participate in, such as code reviews, threat modelling, or security testing.
  - Encourage collaboration with other security champions and relevant teams to address security challenges and share knowledge.
- Communication and Reporting:
  - Explain the communication channels and platforms for sharing security-related information, updates, and resources.
  - Establish regular reporting mechanisms for security champions to share their activities, challenges, and successes.
- Rewards and Recognition:
  - Outline the rewards and recognition system for security champions, such as certificates, badges, or public acknowledgments.
  - Highlight the career development opportunities that may arise from participating in the program, such as leadership roles or specialized security positions.
- Feedback and Improvement:
  - Encourage security champions to provide feedback on the program structure, content, and effectiveness.
  - Create a feedback loop to address their suggestions and continuously improve the program.
- Support and Resources:
  - Provide access to security tools, frameworks, and libraries that can aid their security efforts.
  - Offer support from the security team or designated mentors who can assist with technical questions or challenges.
- Ongoing Engagement:
  - Plan regular meetings or forums where security champions can interact, share experiences, and learn from each other.
  - Foster a sense of community and promote networking opportunities with other security professionals.
- Metrics and Impact:

<https://owasp.org/www-project-security-champions-guidebook/>

# OWASP Security Champions Guide

Principle – 1: Be Passionate About Security

Artefact: Checklist

- Define metrics to measure the impact of the Security Champions Program, such as vulnerabilities identified, security improvements implemented, or security incidents prevented.
  - Regularly communicate the program's achievements and impact to inspire and motivate the security champions.
- Encourage Innovation:
  - Encourage security champions to bring forth new ideas, innovative solutions, or process improvements related to security.
  - Foster an environment that supports experimentation and rewards creative problem-solving.

## Offboarding

- Security champions will leave the program or company for various reasons. Ask them to recruit a successor to ensure continuity within their team(s).
- Arrange an exit interview to get their feedback on the program.
- Collect their success stories for future reference.