PaCSON
PACIFIC CYBER SECURITY OPERATIONAL NETWORK

PaCSON Capacity Building
Action Plan 2025-2028

Overview

Since 2017 PaCSON members have worked together to make significant strides in lifting cyber security capabilities and readiness across the Pacific. The foundations of PaCSON enable cooperation and collaboration by empowering members to share cyber security threat information, tools, techniques and ideas.

A key part of PaCSON is the Capacity Building Working Group. Over the years, we have seen a rapid increase in the delivery of various cyber capacity building initiatives, which has translated into positive changes at the national level. To help shape future efforts in the Pacific and noting the increase of partners wanting to engage in capacity building efforts, members have agreed to the establishment of the **PaCSON Capacity Building Action Plan 2025-2028**. This resource will signal the needs of the Pacific at a regional level.

We would like to thank the PaCSON Capacity Building Working Group members for their valuable contribution to this Action Plan. The five strategic focus areas will channel our focus, to help build capacity in areas that matter most to our PaCSON members and chart a tangible and measurable way forward. We are grateful this opportunity has also allowed us to look back, in order to move forward, in a purposeful Pacific way, as a region.

Strategic Focus ONE

INSTITUTIONAL GOVERNANCE

ACTIONS

- Work collaboratively with other regional infrastructure to build legislation and regulatory support.
- Readiness assessments conducted yearly to understand national gaps.
- Support the development of national cyber security policies and mechanisms.
- Specific support on building CERTs, national cyber centres and CSIRT functions.
- Enhanced formal information sharing mechanisms.
- Deliver study tours to strengthen understanding of governance processes, cross agency collaboration on cyber related issues.
- Regional SOC with ‘break-glass’ incident response function, supported by relevant partners.

Strategic Focus TWO

WORKFORCE DEVELOPMENT

ACTIONS

- Yearly secondments, internships or scholarship opportunities for PaCSON members.
- Deliver train-the-trainer model training on CERT functions.
- Seek investment in establishing workforce development plans or implementation of initiatives to increase number of staff where resources are low.
- Support for professional certifications or micro-credentials.
- Support for attendance at regional and global conferences/ symposiums.
- Partnerships with academic institutions for training on AI/ cyber security.

Strategic Focus THREE

INCIDENT RESPONSE

ACTIONS

- Specific threat hunt and remediation information and training is provided at a bilateral or regional level.
- Regional tabletop exercises and CTFs.
- Training on incident response tools.
- Incorporation of incident communication and advisory training in every PaCSON related initiative.
- Training in cyber security incident management.
- Creation and implementation of incident response plans and playbooks.
- Explore legal frameworks for cross-border cooperation e.g. sub regions.
- Deployment of PaCSON cyber security team for supporting major events (PIFLM, CHOGM, etc.).

Strategic Focus FOUR

CRITICAL TECHNOLOGY

ACTIONS

- Create opportunities for PaCSON members to engage with technology providers to understand their products. This could include engagement with Amazon and Google.
- Share advice on procuring large scale infrastructure and licenses. This includes understanding what support can be provided at a regional scale.
- Developing regulatory frameworks or processes to support critical infrastructure assets and providers.
- PaCSON may join conferences, host side events, or have an AGM together with Vendor Expo or Pacific Cyber Drill.
- Receiving advice from trusted partners regarding equipment/ critical infrastructure.
- Training on a secure by design/ secure by default framework.

Strategic Focus FIVE

REGIONAL UPLIFT

ACTIONS

- Identify ways to continue the deployment of a Pacific technical team to support regional events and forums.
- Support representation at global international forums/ conferences and relevant cyber weeks.
- Provide relevant information to the Pacific Island Forum on cyber security matters for leader’s consideration.
- Deployment of child exploitation filters at a regional level through Internet Service Providers (ISPs).
- Empower/ mandate PaCSON members to implement changes quickly at the national level.
- Reaffirm PaCSON as a part of the regional architecture.