Extracted from NFV(20)000273 approved on 2020.12.18

# Terms of Reference for the Security Working Group (NFV SEC WG)

## Responsibilities

The main responsibilities of this working group are:

- Proactively and reactively reviewing all new WIs for likely security impacts
    - Work with rapporteurs on Work Items in other Working Groups through the editing process to ensure that security concerns are expressed.
    - Drive the necessary contributions and/or change requests in other ISG documents and working drafts in order to reflect specific aspects on security.
- Analysing threats to security in virtualized environments and deriving service and security requirements.
    - Performing gap analysis of supporting tools and frameworks for NFV, e.g., Open Source implementations of functional blocks as detailed in the NFV Architectural Framework.
- Identifying and specifying best practice in areas of security for NFV environments.
- Investigating security enhancements for NFV.
- Addressing the tension between service function and privacy; and the impact of trends such as opportunistic encryption.
- Contributing to the security aspects of NFV demonstrators / proofs of concept.
- Work with external security experts and accreditation institutions to highlight the importance of NFV and encourage involvement.

## Areas of activity / scope

The areas of activity include:

- Information, network and communications security, including resilience, availability and performance isolation of NFV systems.
- Security of individual machines/processes and the security of large systems and networks.
- Security tools, controls and techniques to ensure security in an NFV environment.
- Security at design-time, deployment-time and run-time.
- Appropriate measures for operational efficiency and features to support regulatory requirements, e.g. Lawful Intercept, Privacy and Data Protection.