**How to play – NFR Card Game, and STRIDE**

**The NFR Card Game:**

The technique provides a set of cards which allows a gamification approach to ensure that the developers are considering and addressing the Security requirements. You can see an overview of the process by watching this short video:

https://www.youtube.com/watch?v=6sxq8ldtZ9M

How to play:

1. During backlog refinement (or a dedicated NFR Card Game session can be created), one NFR Card is given to each team member present in the session.
2. One player acts as the facilitator, and uses JIRA (or Trello etc) to open up a User Story on the board.
3. The team discuss the scope of the User Story so everyone has an understanding of what is being achieved (any previous actions taken to achieve this User Story are not in scope for analysis, only the individual User Story on the board).
4. Each player in turn reads out the title of their single NFR Card, and then calls out any applicable NFRs they have on their card.
5. If there are applicable NFRs, the facilitator tags NFR\_IMPACT=YES into the tag field in JIRA, and any applicable NFRs that were identified (e.g. VL.01)
6. If there were no applicable NFRs, the facilitator tags NFR\_IMPACT=NO.
7. After all players have played their single card, the round is over. Each player gives their NFR Card to the person on the left.
8. The next User Story is opened on JIRA, and the steps above are repeated for each User Story.

**STRIDE**:

STRIDE is a threat model developed by Microsoft for thinking about computer security threats. Its name is a acronym for the security threats it addresses, with six categories;

- Spoofing of user identity

- Tampering

- Repudiation

- Information disclosure (privacy breach or data leak)

- Denial of service (D.o.S)

- Elevation of privilege

You can see an overview of STRIDE in action by watching this short video here: https://www.youtube.com/watch?v=wL59RopnnOs

How to play:

It is recommended to play 1 hour of STRIDE per week in a dedicated session as part of the team’s Sprint Cycle, with all team members and any interested members of the client team invited to participate.

1. In the first session, the team draw up a high-level diagram of the designed system.
2. The STRIDE (Elevation of Privileges) Cards are distributed evenly between participants.
3. One player acts as the facilitator, and will track the played cards in a STRIDE Output Document (a template can be found here in github).
4. Each participant takes it in turn to attempt to apply their STRIDE card against the system (Elevation of Privileges suite trumps all others, and Ace high).
5. Once the STRIDE card deck has been completed, a risk assessment should be carried out against each applicable vulnerability that was identified during STRIDE. These should be given a Probability and Impact risk rating, with any User Stories raised to mitigate this resulting in a Residual risk rating.0