**********WORK IN PROGRESS**********

Welcome

Welcome to the information security champion training and basic assessment curriculum. The current working title for this project is OctoC - Curriculum for Creating Cyber-Security Champions and Compliance Checking in Civil Communities (***Yes we know we used the word "Cyber" but the acronym was tricky to think up - open to better suggestions! :)***).

Who is this curriculum for?

This curriculum is designed as a tool for trainers working with people within small NGOs and media organisations who find themselves tasked with the management of the day to day running of secure and private information.

Often these individuals are described as "champions." These people begin this often informal role by being the office "techie" or "printer-fixer" - a person who might not have received formal training before but find themselves dealing with many of the day to day information security concepts.

Though most of the learning will be hands-on and participants won't need to be technical specialists to understand, this course is primarily about taking people who already understand some core concepts and giving them more skills to be able to manage more effectively.

At a minimum, we suggest that participants already have a basic knowledge of tools and techniques listed in or already conducted training similar to the content found resources such as:

- Level-Up
- Security in a Box
- Surveillance Self Defence
- Umbrella App

Why create this course?

This course was created to help fill an identified need within the trainer community. We currently have many resources available for educating users (such as Level-Up), for implementing issues of organisational security (OrgSec community) and for auditing an organisation's security (SAFETAG). What we were missing though, was a curriculum to help people begin to learn how to manage an organisation's information security. That is what this curriculum aims to provide.

How does it work?

The range of knowledge needed to manage information security is enormous and often outside the realm of what any individual could master even with years of training. As such, the curriculum is designed to:

- Introduce individuals to a topic
- Develop a familiarity with key approaches to dealing with the topic within their environment through class interaction and hands-on research
- Leave a topic with a basic knowledge, resources and a developed support network that they can utilise for implementation at a later stage.

Throughout the course, each participant also conducts a basic assessment of their own organisation that they build on for each module that they cover. This helps to a participant to maximise the utility of the course to their own circumstances and leave with an action plan for implementation at a later stage. So for example, a module on privacy will introduce some core concepts, then individuals conduct group work on what's relevant for their individual circumstance, assess how their own organisations deal with the issue and then record this and recommended actions in their assessment for use at a later date.

This trainer curriculum follows the standard pedagogy approach to adult learning adopted by many within the information security training community - such as Level-Up.

This breaks down each lesson into the following five areas:

- Activity - a learning task for the group to conduct
- Discussion - about the module
- Inputs - related lecture or background material
- Deepening - the hands-on portion of the module
- Synthesis - summary and wrap-up. For this curriculum, this is also where participants fill out the assessment.

Trainers should consult "Recommended Preparations" before presenting each module. Most require secure WiFi. Remind participants to bring devices and chargers.

How long does it take?

The course is designed to be modular. Each module comes with a suggested time. Allowing individual modules to be taken alone or a full course to be run. How long the course takes depends on many factors such as language, existing skills etc. However, we aim to make the entire course last at most five days.

What does it cover?

It is not just about digital issues but also addresses things such as the security of physical information like paper documentation. We also discuss the important issues of how to design projects to ensure responsible collection of data and the ensuring privacy by design within projects.

The course is broken into the following sections:

- Introduction
- Mapping information, assessing the threat environment and modelling
- Privacy regulation and requirements
- User Education
- Encryption, Patching, Licensing
- Network Management, Monitoring, WiFi and Logs
- Communications
- Web and Email Management
- Password Management
- Mobile Device Management / BYOD
- Travel
- Resilience and Backups
- Policy Creation and Implementation
- Physical Security
- Responding to Incidents
- Basic audits
- Community structures and resources for further learning

Licence