

WebF1 Worksheet: Web Security

For this task, you should form groups of between two and four people.

Your group should consider the information that is generated by you on a daily basis, how it is captured, how it is shared and how it can be secured. In doing this, you should consider the confidentiality of the information, the integrity of the information and the availability of the information.

Your end result is to produce a strategy that a future social media network could adopt.

This policy should cope with receiving manually entered information as well as automatically gathered data on your wider online activity and from Internet of Things (IoT) devices. A key requirement for the policy is that users are able to have a fine-level granular control over the security associated with their information. The language used to describe this security should also be easily accessible.

Task 0: Keep a log of what you do

- Use the Discovery Log you started last week to continue to record what *you* learn during each task, paying special attention to the things you are learning from your peers during your discussions. Peer-learning is critical to your success in Higher Education (HE).

Task 1: Work Collaboratively

- One group member should create a Google Doc.
- Title the doc "WebF1 Security Policy Task".
- Share the doc with each member of the group, giving everybody editing rights.
- Use this document to work collaboratively on your ideas.

Task 2: Identify all information

- You should begin discussions by listing all the different kinds of information that you generate on a day to day basis.
- As a part of the process of listing this information, you should also consider how this information is, or could be, captured and input into your final system.
- Record what you identify in your "WebF1 Security Policy Task" document.

Task 3: Categorise that information

- Once you have identified all of the information that a person generates (or causes to be generated) on a day-to-day basis, you should begin to design a set of categories that this information falls into.
- These categories could be traditional “secret”/“sensitive”/“public” or they could be based on the confidentiality/integrity/availability triad (i.e. you can have multiple categories for different levels of encryption, for how information integrity is checked and maintained and for how information is made available).
- Your categories should be easy for all users to understand.
 - i.e. Do not specify algorithms, key sizes or other technical detail.
- Record your categories in your “WebF1 Security Policy Task” document.

Task 4: Processing information

- How will a future social media service associate new information with the categories you have defined?
 - i.e. Define how information might be received and classified.
 - Think about the different data sources: manual, third party, IoT, etc.
- Record your definition in your “WebF1 Security Policy Task” document.