











Session 9	<b>Information Security &amp; Privacy</b>		 Duration: <b>30 mins</b>
<p><b>Session Summary</b></p> <p>This session looks at the risks of data loss and examines vulnerabilities related to the way information is managed, and the use of social media.</p>			
<p><b>Session Objectives</b></p> <p> <ul style="list-style-type: none"> <li>• Highlight risks associated with gathering, storing, and disseminating sensitive information.</li> <li>• Outline different methods and practices for securing information.</li> <li>• Examine digital footprints and consider the security risks associated with using social media.</li> </ul> </p>			
<p><b>Learning Outcomes</b></p> <p>By the end of this session participants should be able to:</p> <p> <ul style="list-style-type: none"> <li>• Recognise the risks associated with managing information and using social media, and list measures to protect sensitive information.</li> </ul> </p>			
<p><b>Supporting Material</b></p> <p> <ul style="list-style-type: none"> <li>• <a href="#">GISF The Information Management Challenge: A Briefing on information security for humanitarian Non-Governmental Organisations in the field.</a></li> <li>• <a href="#">GISF Security to go: a risk management toolkit for humanitarian aid agencies – Module 4.</a></li> </ul> </p>			
Time	Suggested Activities		Resources
2 mins	<p><b>Introduction</b></p> <p>Introduce the session and provide a brief overview of what this session will cover.</p>		<ul style="list-style-type: none"> <li>• S.9 Information Security &amp; Privacy Presentation - Slide 1</li> </ul>
3 mins	<p><b>Sensitive Information</b></p> <p> Ask participants: <i>What sensitive or confidential information do aid organisations gather, store or disseminate?</i></p> <p>After listing the participant's suggestions on a flip chart, refer to slide with examples of sensitive and confidential information. If internal training, adapt list to reflect confidential or sensitive information collated by your organisation. Draw attention to tactics used by repressive governments, armed actor groups, and criminal networks to access information, including surveillance, monitoring and intrusion. Stress the need to be security-conscious when collating, storing, communicating, and disposing of sensitive information.</p>		<ul style="list-style-type: none"> <li>• Slide 2</li> </ul>
5 mins	<p><b>Securing Information</b></p> <p>Explain that securing information requires a combination of three key elements - Physical Security, Digital Security and Communications Security. Provide examples of the different elements that are relevant for the local context, or your organisation.</p>		<ul style="list-style-type: none"> <li>• Slide 3</li> </ul>

	<p> Information security is comprised of a layered approach, with several barriers to protect information from loss, theft and unauthorised access or disclosure:</p> <ul style="list-style-type: none"> <li>• Physical Security - locked filing cabinets, 'clear desk' policies, visitor procedures, secure disposal of documents.</li> <li>• Digital Security - password protection and encryption, restricted access to folders/files, backing-up systems, secure disposal of computers and data storage devices.</li> <li>• Communications Security - secure communication practices, splitting information, using secure email and file-transfer systems.</li> </ul> <p>Highlight that measures need to be proportionate to the sensitivity or confidentiality of the information being gathered, stored or disseminated, and the risks that exist in that context.</p> <p> Excessive procedures can be burdensome on staff and therefore will not be complied with or can generate unnecessary attention and suspicion from the authorities.</p>	
5 mins	<p><b>Digital Footprint</b></p> <p>Briefly discuss the impact our digital/online footprint has on our security and safety, and explain how this information can be used against us by criminals or by other groups to harass, threaten or arrest aid workers. Highlight any recent incidents/examples from the operating environment, if available.</p> <p> As digital or technology-based risks continue to evolve, we must ensure that we remain aware of the various digital threats that exist and that we adapt our online behaviours to mitigate risks to ourselves, colleagues and the organisation.</p>	• Slide 4
15 mins	<p><b><i>ACTIVITY: Data Mining*</i></b></p> <p>Explain to participants that they are going to be exploring their 'digital footprint' in more detail. Ask for two volunteers who use some form social media and make the volunteers team leaders of two groups. Divide the remaining participants into the two groups.</p> <p>Give each group five minutes to find out as much information as possible about the team leader in the other group. If volunteers are not forthcoming, groups can be asked to gather information on themselves, or both groups can be asked to find out information on the facilitator. The group with the most correct information wins - emphasise that it is a race between the two groups.</p> <p>Information collated may include personal details such as email address, full name, age, address, etc, but also other information such as hobbies or interests, clubs or associations, previous jobs/roles, education etc. Each group should write the information they discover online about the participant on to a flip chart sheet. They should do this out of sight of the other group.</p>	

	<p>After 5 mins, ask each group to reveal the information they have collected. Highlight any aspect of the information collected which could create a security risk – for example their address, political associations, blog posts, former career.</p> <p>Emphasise the need to be conscious of your online footprint and to use privacy settings to manage the personal information that is publicly available.</p> <p><b>*Alternative</b> – in locations with limited data network run a Securing Information exercise. Split participants into 3 groups. Give each group one of the three key elements – Physical Security, Digital Security and Communications Security. Ask each group to identify measures that fall under the different categories that are applicable in the location they are operating.</p>	
5 mins	<p><b>Social Media Use</b></p> <p>Highlight the wide-spread use of various social media platforms, and their benefits for the sector (information source, campaigning, fundraising, etc) and on a personal level. Then explain how its use can also be a source of security risks. Provide examples of situations where aid workers or their organisation have faced security risks because of content or comments individuals have posted online.</p> <p>Outline some of the essential good guidance staff should follow when interacting and posting online to prevent additional security risks for themselves or their colleagues.</p>	<ul style="list-style-type: none"> <li>• Slide 5</li> </ul>