Safety Hour Discussion Pack

Topic: Information Security

Purpose of the discussion:

To discuss why Security is more important than ever.

This discussion pack is to be used to support the security offline briefing. It has been designed to be delivered to staff who are unable to access the security elearning via OLM. The briefing is to be played at the beginning of the safety hour and followed by a discussion around it's contents.

Security training is mandatory for all staff, participation in this security safety hour briefing will fulfil the learning requirement for staff who are unable to complete the security elearning individually via OLM. Therefore it is very important, at the end of the session, for you to update the competencies of those completing the session to record their learning in OLM.

Prepare the offline briefing

- Refer to the 'Presenter guide' to guide you in preparing and recording this briefing http://connectdocs/NetworkRail/Documents/CorporateServices/InformationManagement/InformationSecurity/Security%20training/Information_Security_Briefing_Presenter_Guide.pdf
- You will need a projector or a screen to allow participants to view the briefing.
- Complete the 'Information security' elearning via OLM yourself.
- Download the off line version of this briefing in advance of the session by searching on OLM for 'Information Security (Briefing)'. This can take 5-10 minutes to download so please allow for enough time prior to the session.
- Familiarise yourself with the material in the presentation and this pack
- Print a copy of the registration form to be completed for each session to later record the data in OLM.

Kick-off the discussion

Open the session stating that;

'Security is everyone's responsibility, even if you don't use a computer as part of your daily routine – as you'll see, security isn't just about computers. This briefing and discussion will give you the knowledge you need to stay secure.'

Play the application: Information_Security_Briefing

Record in OLM

Completion must be recorded on the Oracle e-business suite in Competence Profile via 'Competence Manager NR' for staff in attendance.

Safety Hour Discussion Pack

Topic: Information Security

Discussion points: Use below to plan your facilitated discussion. Remember, you don't have to have all the answers – the role of the facilitator is to create an engaging discussion where everyone identifies and commits to solutions.

Discussion points	Supporting notes

Take responsibility:
 	
Did anyone tailgate you today into the workplace?
	Let the team brainstorm how they can protect themselves and colleagues and property.
	
	Questions:
	• Did anyone tailgate you into the workplace this morning?
	
	• Have you let anyone that doesn't work for Network Rail (rail workers)? How do you confirm they are who they say they are and have the authority to enter?
	
	• What about the local sandwich van or pizza company? Have you ever let them in or left gates open for food vans to come in, or shared access codes?
	
	Key messages here are:
	
	• **Leaving gates and doors open** – presents a serious security risk. This could allow unauthorised people to access restricted areas putting both security and safety at risk including harm to people and damage to the infrastructure.
	
	• **Take responsibility** – help protect our railway against criminal acts such as theft and vandalism and general health and safety concerns. Ask yourself, is this secure?
	  ◦ Are gates and doors kept closed and locked?
	  ◦ Is lighting acting as a security measure or would it assist an intruder?
	  ◦ Are boundaries secure? Are vehicles or other property left in places that could assist fences be scaled / climbed?
	
	If challenging suspicious behaviour do remember that your personal safety is paramount.

Safety Hour Discussion Pack

Topic: Information Security

Discussion points	Supporting notes
Behave securely: What are the risks with sharing passwords?	**Let the team brainstorm how they can protect our information and systems.** You wouldn't leave your payslip just lying around. Some information you want to keep private. The same applies for our data - like employee data or commercial contracts, route information and financials – we need to keep secure. Is there anything they currently do, or don't do, that could make us vulnerable to an attack? • Do you share passwords? • Do you share passwords for generic accounts? • Do you know you're responsible for other's activities if they're using • your account? Key messages here are: • Individual passwords and login in should never be shared. • Generic account passwords should only be shared within the closed group, not written on notice boards or monitors. • Always lock your screen when you're away from your desk, even if it is for a moment. Hit ENTER after, CTRL+ALT+DEL every time you leave your seat or press WINDOWS+L • Never leave mobile devices unattended. If lost or stolen, report immediately **Ask the group to suggest how they might work/behave differently following the discussion.**

Safety Hour Discussion Pack

Topic: Information Security

Discussion points	Supporting notes
Protect our Railway: What is acceptable use or work equipment?	Our policies and standards relate to everyone, they are there to protect us. Let the team discuss: • Do you know what is acceptable use of work equipment? Keep your work and private life separate. • What data do you have access to that could be a security risk in the wrong hands? This could be our personal data or sensitive data about special trains. Key messages here are: **Follow company policy and standards** – make sure you know the rules on email, social media, mobile devices etc. There are people you can ask if you are unsure. **Protect company information** – be careful how you handle removable media (USB sticks), think about what information you're emailing – is that the most appropriate way of sharing information?

For further information:

Contact the Security team: AskSecurity@networkrail.co.uk

Search 'Security' on connect or visit the Information Security group on Yammer #AskSecurity

Do you know who your local Security Champion is? Contact securitychampions@networkrail.co.uk or visit the Security Champion group on Yammer #securitychampions