JV REP WORKSHOP

Cyber Security – What do we say?

JIG MTF Rome

Note: *The procedures and practices presented in this document are best practice recommendations only. JOINT INSPECTION GROUP Ltd and/or the JIG Member presenting this document makes no claim or warranty whatsoever as to their completeness or suitability. JOINT INSPECTION GROUP Ltd and its Members shall have no liability to third parties in relation to following, or not following the recommendations contained herein.*

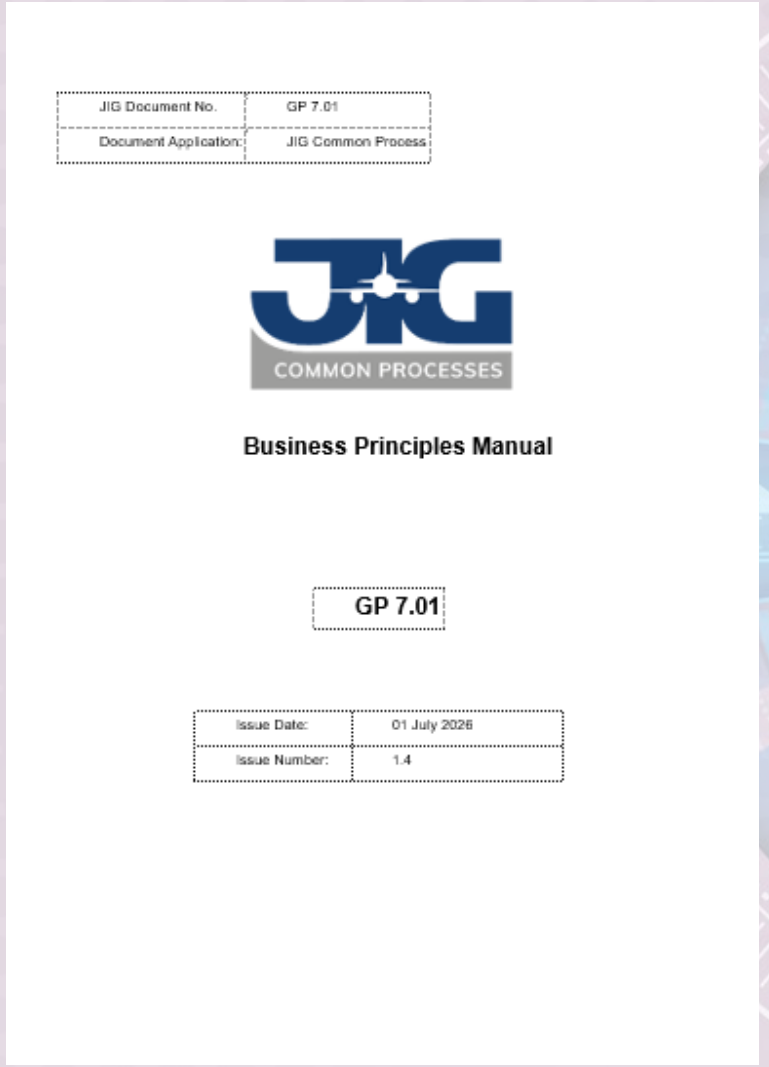
First a case study

- Hackers accessed the Manage My Health (MMH) online portal used by healthcare providers to share information with patients.
- The health records of nearly 100,000 people were stolen by the hackers, who demanded payment of a US$60,000 ransom.
- Hackers accessed the Manage My Health portal by using valid user credentials. They gained entry through the "front door" of the system.

The investigation highlighted key governance issues

- Outsourcing services does not outsource accountability. “Simply relying on vendor assurances about their security profile is problematic”. Robust due diligence is essential.
- Privacy and security expertise is key to good privacy governance and oversight. And good governance is critical to understanding and managing privacy and security risks.
- Privacy impact assessments are essential tools for understanding privacy risks.
- Appropriate contractual safeguards need to be in place when engaging third-party providers to handle data.

Information Security / Data Protection



JIG Document No.	GP 7.01
Document Application:	JIG Common Process

COMMON PROCESSES

Business Principles Manual

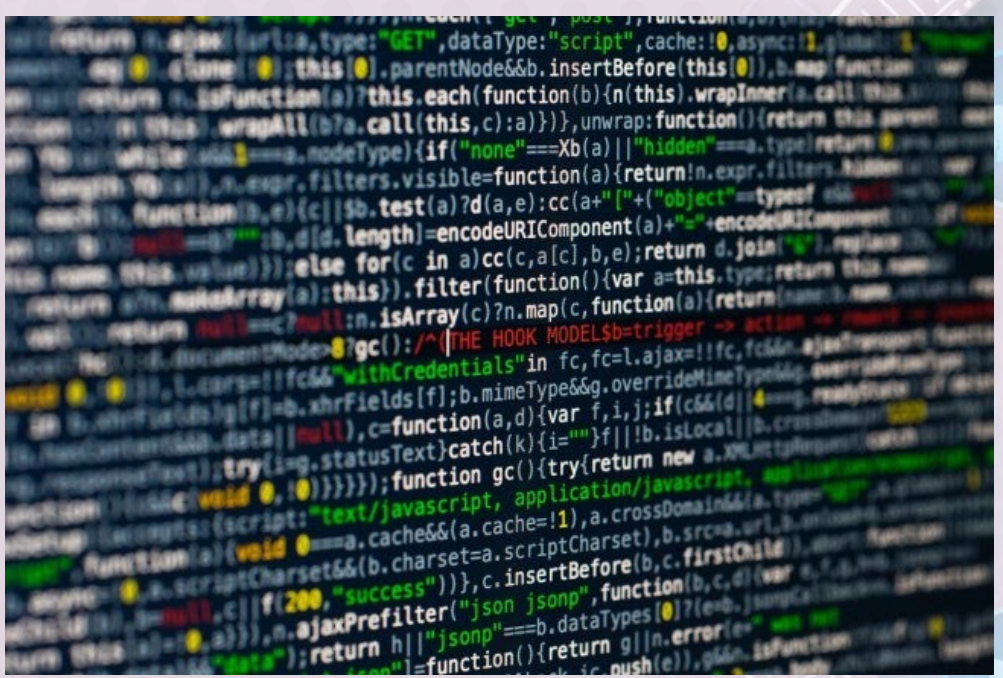
GP 7.01

Issue Date:	01 July 2026
Issue Number:	1.4

Our Business Principles:

- Protect Entity, participant, user & customer information
- Pre-plan responses in the event of a data breach or cyber-attack
- Protect digital systems

Protect Entity, participant, user & customer information



- Restrict access to Confidential information and IT systems to the minimum levels of access and privileges required to perform a function or role.
- Formulate and operate an internal governance framework for Digital Security of Digital Technology.
- Establish and maintain risk management processes to identify, assess and manage risks to Confidential Information and IT systems.
- Ensure that subcontractors protect participants, user and customer data and systems.
- Ensure vendors / suppliers comply with the Entity personal data protections requirements.

Pre-plan responses in the event of a data breach or cyber-attack

- Establish plans that detail how the Entity should respond, what the Entity's regulatory obligations are and who they should engage with in the event of a data breach.
- Establish a notification protocol in the event of an incident that notifies other participants and users that may be at risk.
- Agree the actions that a participant or user should provide.

Protect digital systems

- Ensure users of the Entity's or Entity Participants' digital assets know how to keep them secure.
- Comply with all the applicable Digital Security laws and regulations.
- Create and maintain a Cyber Security Function (can be an internal or external party).
- Implement procedures that structurally assess and measure Digital Security risk factors and implement measures to address and remediate those risks.
- Develop procedures and measures for Identity and inventory management and Protection of Digital Technology.

What do you have in place?

- Do you know what the worst case scenario is if you have a cyber security breach?
- Is cyber security on your risk register? Is this discussed at your JV Committee meeting?
- Have you performed a gap assessment against the BPM practices?
- Have you tested your cyber security plans recently?

Thank you!


Q&A