SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

# PHYSEC1: Annex Table 4 – *Physical security for specific types of ICT equipment*

| Specific ICT equipment | Physical security requirement |
|---|---|
| **Solid state drives or hybrid hard drives** | Solid state drives and hybrid drives cannot be made safe through normal data wiping processes when switched off. It is **recommended** that agencies using equipment with these drives seek advice from ASD on methods to secure this equipment (e.g. encryption) |
| **Deployable ICT systems** | Physical security measures may be difficult to apply when using deployable ICT systems, particularly in high-risk environments. It is **recommended** that agencies seek advice from ASD on suitable controls to help mitigate any risks from using deployable systems. |
| **Network infrastructure** | Protection of network infrastructure requires a combination of physical security measures and system encryption. If the encryption used is approved by ASD, the physical security requirements can be lowered in accordance with the Australian Government Information Security Manual (ISM). For information on the protection of network infrastructure, see SAPSF policy Robust ICT and cyber security.<br><br>Tampering of network infrastructure is a security risk. It is **recommended** that agencies secure network infrastructure equipment (e.g. patch panels, fibre distribution panels and structure wiring enclosures in containers and secure rooms. If this is not possible, it is **recommended** that agencies meet the system encryption requirements of the ISM. |
| **ICT system gateway devices** | Unauthorised access to gateway devices is a security risk. It is **recommended** that gateway devices are located within dedicated ICT facilities. Guidance for securing ICT system gateway devices is available in the ISM. |