Data Security and Privacy - Principles

When implementing a data management system, your government should take into account the following principles in order to protect the security and privacy of the data:

Principle	Consideration
Least Privilege	• Access to a system for a user or group of users should only maintain the minimum necessary rights and privileges needed to perform the task. Limiting privileges limits harm that can be done to the system. • Least privilege is also known as *additive permissions:* all users start at the lowest/most restricted level of access, and new permissions are added as required.
Fail-Safe Defaults	• When a system or process fails, it must do so in a safe way. • *Deny access* is the industry-recommended default position, so that if there is a failure in the system it will not inadvertently expose data.
Economy of Mechanism	• Use simple solutions when available. If a solution is too complex, user acceptance may be low. • From an implementation perspective, complex mechanisms are more difficult to audit and verify for correctness.
Complete Mediation	• Every request should be verified. This includes requests for both digital and physical assets. • All operations go through protection mechanisms; all aspects of the process must be addressed. For example, if some data is collected electronically and processed automatically with inline security checks, then when the

	same type of data is collected on paper and processed manually, it must undergo the same security checks.
Open Design	• Security mechanisms need to be open, evaluable, and based on industry standards. • The protection of data and the system should not rely on the secrecy of the protection mechanism itself. • Do not use in-house designed protection mechanisms which may suffer from lack of complete testing and potential access loopholes. This can lead to an increased change of data loss or system breach. Using open, industry accepted protection mechanisms means that they have been reviewed and tested.
Minimization of Risk	• Wherever possible, remove personal identifiers and anonymize data. • Unnecessary data should always be deleted.
Least Common Mechanism	• Mechanisms that are used to access resources should be dedicated as this prevents potential crossover between channels in the event of a failure.
Psychological Acceptability	• Analyze and understand how security controls are used and viewed by users. Overly complex measures may result in low user adoption or push back.
Defense in Depth	• A comprehensive data security strategy is formed by utilizing multiple different layered techniques with an overall goal of working to protect the system and data. • With multiple independent defense strategies in place, failure points are decoupled which means that if there is a failure of one component, other protection services are unaffected. • Multiple independent defense points lead to a stronger system than a system where all defense points are linked. • When considering a solution and developing a data management plan, an organization must consider using a

	diversity of defense strategies that cover all aspects of their system, not just the data itself. This includes: ○ the network by which machines are connected ○ host security such as user workstations or access portals ○ physical resource protection, both in terms of limiting access but also disaster prevention for fire, power and flood protection • For each component, protection mechanisms need to be applied using a layered approach and should be dissimilar. If a system is compromised at one point, the knowledge of how to get around those specific security measures will not be useful as other protection mechanisms will use different strategies.