

## Information Security Policy Assessment Checklist

No	Procedures	Status	Notes
1	Is there an executive directive/statement to ensure there is an information security architecture that includes risk, governance, ethics, compliance, privacy, and protection of enterprise assets? Are enterprise roles, responsibilities, and accountabilities defined? Are the executive team and the board of directors on the same page?		
2	Are there data/information requirements stating that it must be available, accessed by need to know or have, and in the most accurate format?		
3	Are staff required to acknowledge policies on new hire and termination, and at regular intervals? Are the staff types of enterprise network access defined? Is an enterprise asset defined?		
4	What types of services and applications are permitted on the enterprise network, who is permitted to perform the installs and removals, and who is permitted to perform the monitoring? How are connections (hardwired, wireless, remote) defined to the enterprise network?		
5	How are access roles, accountabilities, and responsibilities defined for network, applications, and devices? How are monitoring, logging, and reporting defined for goals and objectives?		
6	Who is permitted onsite and permitted to plug what type of device into the enterprise network? What is the standard authorization and authentication mechanism for the enterprise?		
7	How are staff going to request access to a network, application, device, or service, who will grant access, and who will be required to monitor logs and access? How do staff access the building, business areas, and communication rooms? Is electrostatic training required for anyone who enters a data center? Is the building segmented by badge control?		
8	How are incidents/exceptions reported, to whom are they reported, how are incidents/exceptions reviewed? (These are not necessarily security breaches.)		
9	How are the enterprise network devices configured? How are they monitored and put back into compliance? What is the exception process to the standard? Are all ingresses and egresses documented within the enterprise?		
10	If something happens in the enterprise environment, how is it reported and how are systems and information recovered?		
11	Is there an asset and information classification matrix and are the risks defined for the asset classification? Is there a statement about the protection of the enterprise assets?		
12	Within the information security team and operational duties is there a document listing the segregation of duties and responsibilities, so no one person has the responsibility of complete end-to-end transaction processing?		
13	If the enterprise should happen to lose its information security team, are there enough details and documents to permit a third party or another business unit to take over the duties and continue the business until the team is replaced?		
14	Is the location of all documents documented and known to all staff members? Is there a document management system? Is there a review process and an owner assigned to each document?		