**Overview of policies to review/consider for cybersecurity testing**

**Acceptable Encryption Policy**

Acceptable encryption policy provides guidance and limits to the use of specific encryption algorithms. It also helps ensure compliance with federal, state and international regulations.

**Acceptable Use Policy**

Acceptable use policy to describe the acceptable use of computer equipment in your company. These rules protect both, the worker and your company.

**Clean Desk Policy**

Clean Desk Policy sets the minimum requirements for the maintenance of a “clean desk", so sensitive information about our employees, intellectual property, customers and suppliers is secure and stored out of sight. A Clean Desk policy not only complies with ISO 27001/17799 but also with GDPR.

**Data Breach Response Policy**

The data breach response policy sets out the goals for the breach response process. This policy clearly defines a data breach, the roles and responsibilities of employees, reporting standards and metrics, remediation and feedback mechanisms in case a breach occurs.

**Disaster Recovery Plan Policy**

The Disaster Recovery Plan Policy defines the recovery process for IT systems, applications, and data in case of any disaster that causes a system failure.

**Digital Signature Acceptance Policy**

The Digital Signature Acceptance Policy is intended to provide guidance on validating a signer's identity in your company's electronic documents. Since communication is mainly electronic, the aim is to reduce confusion about the trust of a digital signature.

**Email Policy**

The email policy sets the minimum requirements for the use of emails within your network of companies.

**Ethics Policy**

The ethical policy is to create a culture of openness, confidence and emphasize the expectations of fair business practices. Practical ethics is a team effort involving your company's employees.

**Pandemic Response Planning Policy**

Pandemic Response Planning Policy provides directions and disaster recovery procedures to plan for and prepare for the rare event of a pandemic disease outbreak. The objective is to address the fact that pandemic events can create problems beyond the scope of traditional staff and technology planning.

**Password Construction Guidelines**

The Password Construction Guidelines are designed to provide best practices for strong password creation.

**Password Protection Policy**

The Password Protection Policy establishes a protection standard for distributing and storing passwords.

**Security Response Plan Policy**

The Safety Response Plan policy requires that all business units develop and maintain a safety response plan. This ensures that the security response team has all the necessary information to respond effectively to a safety incident.

**End User Encryption Key Protection Policy**

The End User Encryption Key Protection Policy sets out the protection requirements for end-users with encryption keys. These requirements are intended to avoid unauthorized disclosure, negligence, and wrongful abuse of encryption keys.

**Acquisition Assessment Policy**

Acquisition Evaluation Policy defines the minimum-security requirements for an Infosec acquisition evaluation.

**Bluetooth Baseline Requirements Policy**

The Bluetooth Baseline Requirements Policy provides a minimum standard to connect Bluetooth devices to the network devices of your company. The minimum standard shall protect personal data and critical company information.

**Remote Access Policy**

The Remote Access Policy lays down the rules and conditions for connecting any host to your company's network. These rules and requirements are intended to reduce the potential risk of damage to your company due to the unauthorized use of your company resources.

**Remote Access Tools Policy**

The Remote Access Tools policy applies to all tools used for remote access connections from your company's equipment.

**Router and Switch Security Policy**

The Router and Switch Security Policy describes the minimum-security configuration required for all routers and switches connected to or used on behalf of your company in production capacity.

**Wireless Communication Policy**

Wireless Communication Policy is to maintain the confidentiality, integrity, and availability of all communications connected to your company's wireless network.

**Wireless Communication Standard**

The Wireless Communication Standard sets out the technical requirements for connecting wireless infrastructure devices to your company network.

**Database Credentials Policy**

Database Credentials Policy sets out the requirements for a program to access a database running on one of the networks of your company.

**Technology Equipment Disposal Policy**

Technology equipment management policy defines the guidelines for disposing of your company's equipment and components.

**Information Logging Standard**

Information Logging Standard is to identify the specific requirements for access logs and audits management of a company.

**Lab Security Policy**

Lab Security Policy sets out information security requirements to help manage and safeguard laboratory resources by minimizing the threat of data exposure to unauthorized accessors.

**Server Security Policy**

Server security policy is to set the basic configuration standards for the servers and data storage equipment of your company.

**Software Installation Policy**

The software installation policy describes the software installation requirements on company devices.

**Workstation Security (For HIPAA) Policy**

The Workstation Security Policy ensures compliance with the requirements of the HIPAA Workstation Security Rule 164.310(c).

**Web Application Security Policy**

The Web Application Security Policy defines the security assessments of web applications within your business.