FORTRA™

TECH NOTE (TRIPWIRE)

Complying with NIA

Keeping sensitive data and assets safe is the goal of regulatory cybersecurity frameworks such as the NIA. The National Information Assurance Policy provides organizations with the necessary foundation and the relevant tools to enable the implementation of a full-fledged Information Security Management System.

The NIA policy guides organizations in classifying the impact of information security threats (and risk), as well as the selection of suitable mitigating controls, with the goal of:

- Protecting information assets
- Effectively manage information security risks
- Achieving regulatory compliance
- Easing the compliance journey for international standard certifications (ISO 27001 and others)

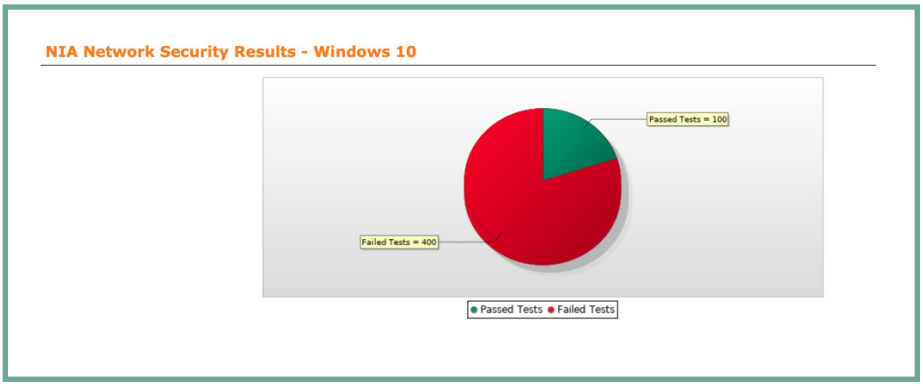
The NIA policy is applicable in all business contexts to support national and/or sectoral compliance requirements. But for security professionals, staying compliant can be difficult due to the complexity of applying the controls, especially without the right cybersecurity tools.

This policy specifies high-level information classification and also focuses on system information and integrity for entities in the State of Qatar.

The Security Controls of NIA cover mainly technical control areas that need to be implemented as baseline security. The following pages show how Fortra's Tripwire solutions map to those controls.

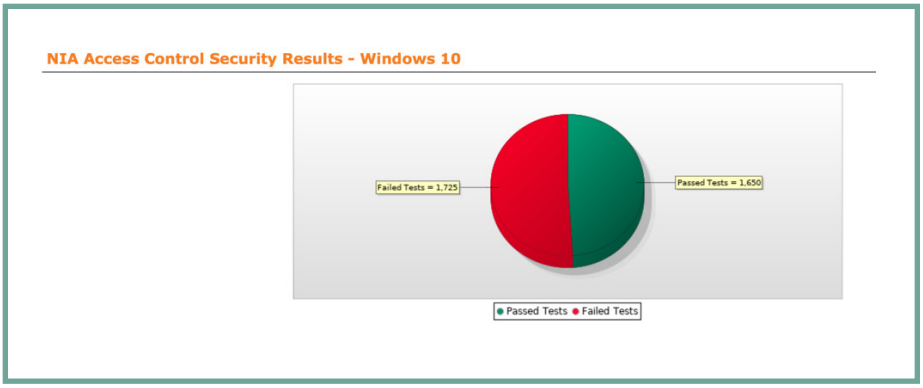
Network Security (NS)

This policy establishes the baseline for the general use and connection of IT networks.



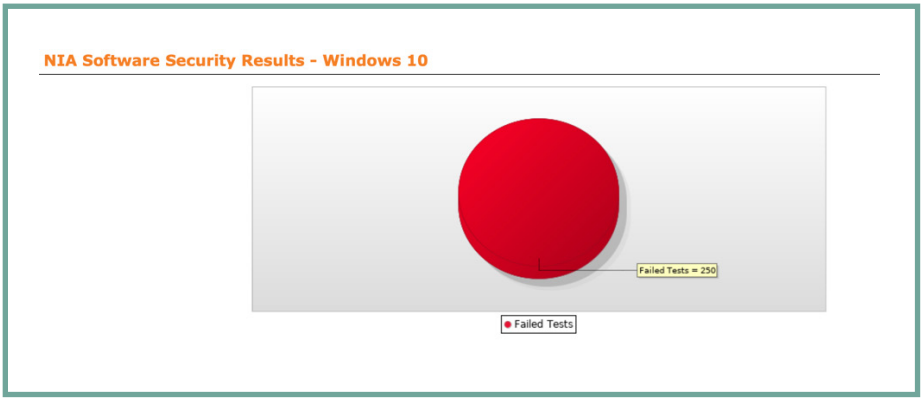
Access Control Security (AM)

The objective of this policy is to establish the use and deployment of a variety of access control solutions to ensure the confidentiality, integrity, and availability of the Agency's information assets.



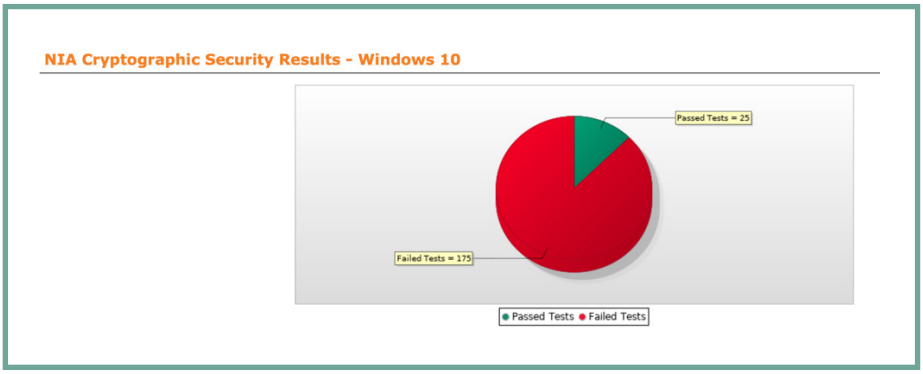
Software Security (SS)

The purpose of this policy is to define the importance of including security in the process of software development and acquisition, rather than treating it like an add-on.



Cryptographic Security (CY)

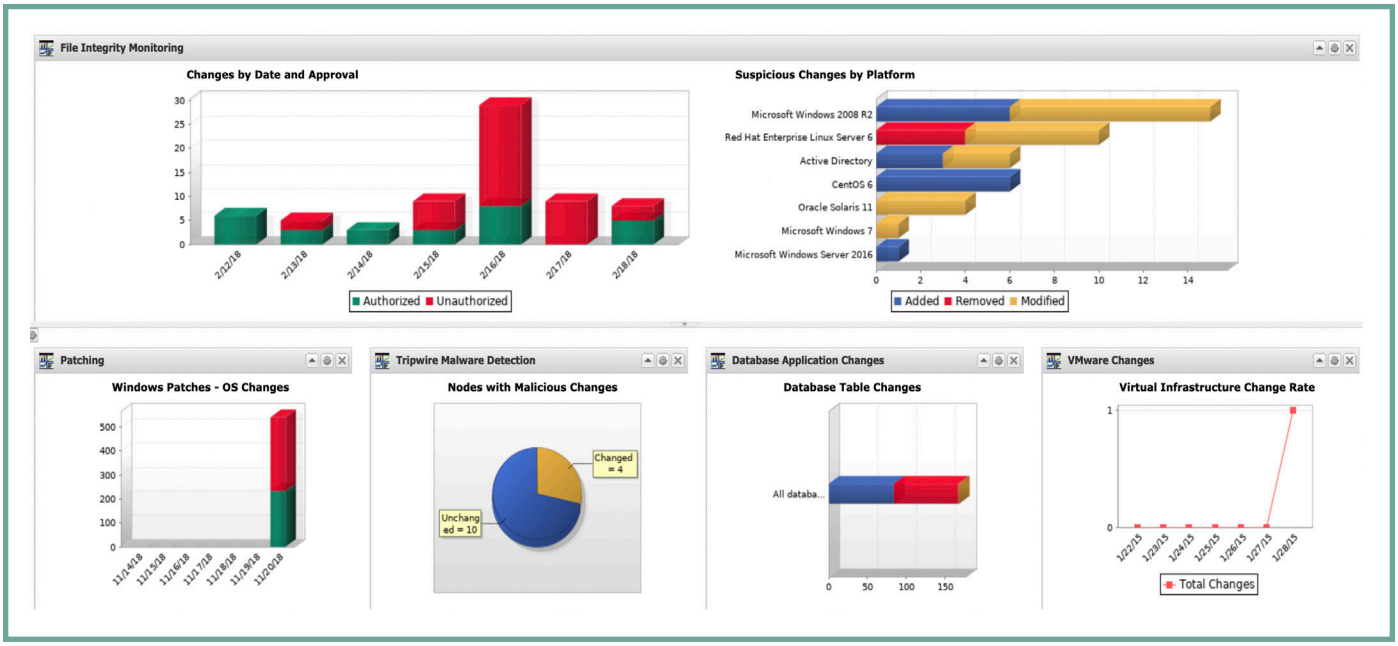
This policy establishes the baseline for the use of encryption technologies for keeping information assets confidential and/or maintaining their integrity.



In addition, NIA policy requires integrity checks of all servers, the regular review of system security, system audit trails and logs, and confirmation of the state of system configurations.

Tripwire® Enterprise is a security configuration management (SCM) suite that provides fully integrated solutions for policy, file integrity and remediation management. Organisations can use these solutions together for a complete end-to-end SCM solution, or use its file integrity monitoring or policy management solutions on their own to address today's pressing security and compliance challenges—while building a foundation that positions them to address tomorrow's.The suite lets security, compliance and operations teams rapidly achieve a foundational level of security across your entire enterprise, including on-premise, cloud and industrial assets, by reducing the attack surface, increasing system integrity and delivering continuous compliance.

Tripwire has taken its original host-based intrusion detection tool, which could simply detect changes to files and folders, and expanded it into a robust file integrity monitoring (FIM) solution, able to monitor detailed system integrity: files, directories, registries, configuration parameters, DLLs, ports, services, protocols, etc. Additional enterprise integrations provide granular endpoint intelligence that supports threat detection and policy and audit compliance..



Tripwire Enterprise dashboard

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.