titus
by HelpSystems

NCA ECC compliance support that works **for your business**

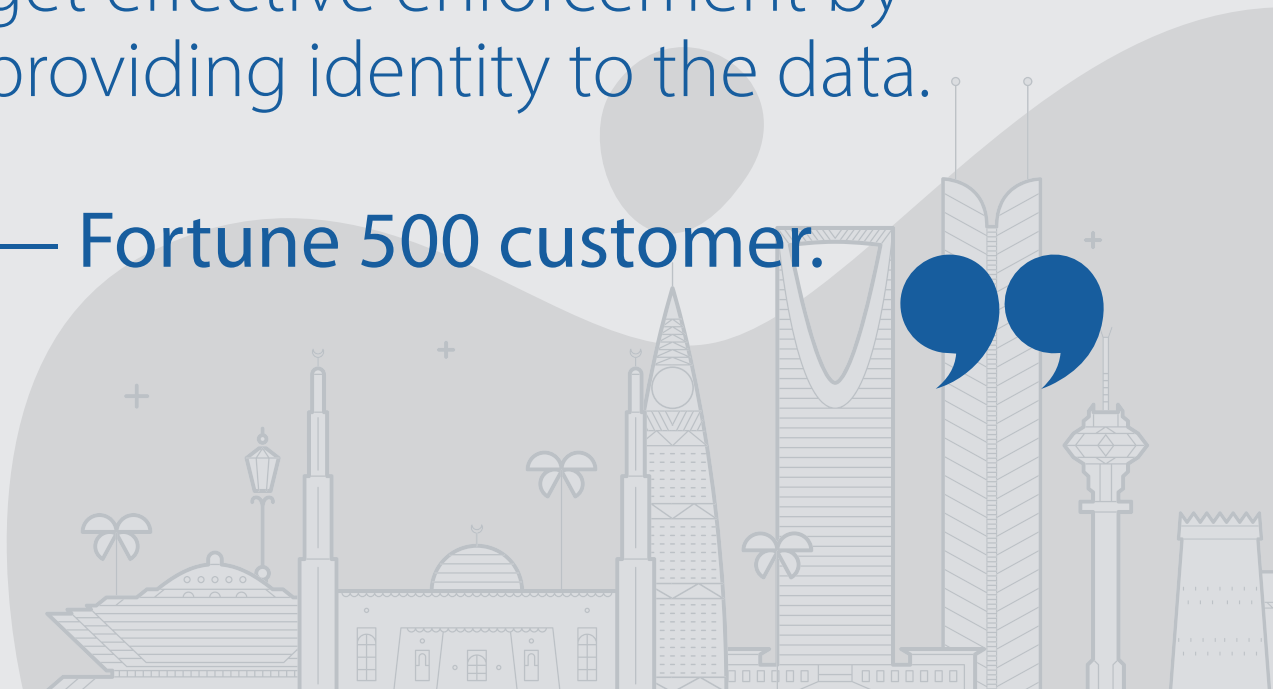
Titus enables government organisations to effectively identify and minimise their cybersecurity risks.

Maintaining the confidentiality, integrity and availability of sensitive data while safeguarding against increasingly sophisticated cyberthreats is an evolving challenge. The National Cybersecurity Authority (NCA) published the Essential Cybersecurity Controls (ECC-1:2018) framework to help government organisations protect their networks, systems and data as well as comply with security regulations and guidelines. NCA ECC-1:2018 mandates a common approach to information security across public sector organisations, their third parties and private companies responsible for critical national infrastructure to help maintain confidence in the sector.

To mitigate information security risks, modern organisations must implement a broad system that will identify personal and sensitive data, understand the context, classify it and protect it across the organisation's entire security ecosystem. Protection must be maintained consistently and efficiently throughout the data life cycle, while data is in transit or at rest, on site and in the cloud.

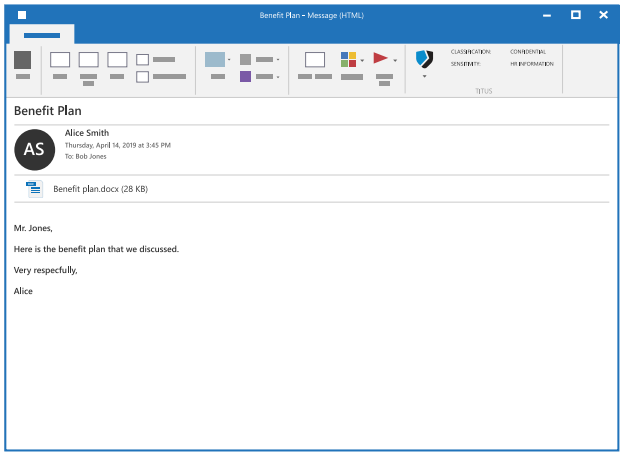
Titus supports your compliance with ECC-1:2018 and helps you meet data protection obligations at home and abroad by complementing and strengthening your existing information security infrastructure.

> We see ROI through prevention. We've calculated that a breach would cost $350 per record. Titus is the vehicle we use to get effective enforcement by providing identity to the data.
>
> **— Fortune 500 customer.**



How Titus supports your **ECC-1:2018 compliance**

Titus works in concert with your existing cybersecurity infrastructure to help you achieve end-to-end cybersecurity compliance. The open, configurable, policy engine enables your organisation to enforce detailed data identification and information handling policies with award-winning machine learning, while monitoring compliance and continuously reinforcing a culture of security.



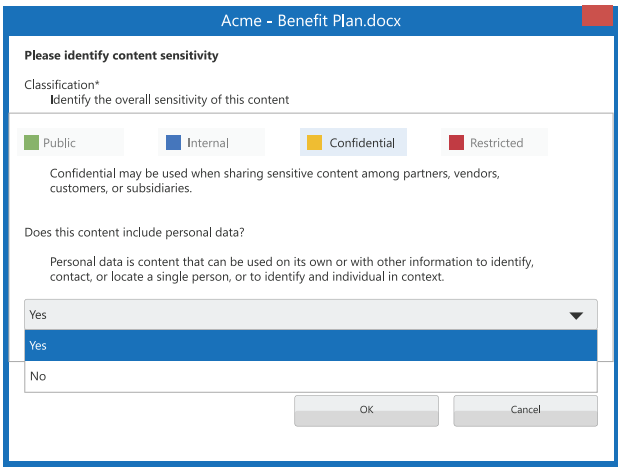
Discover

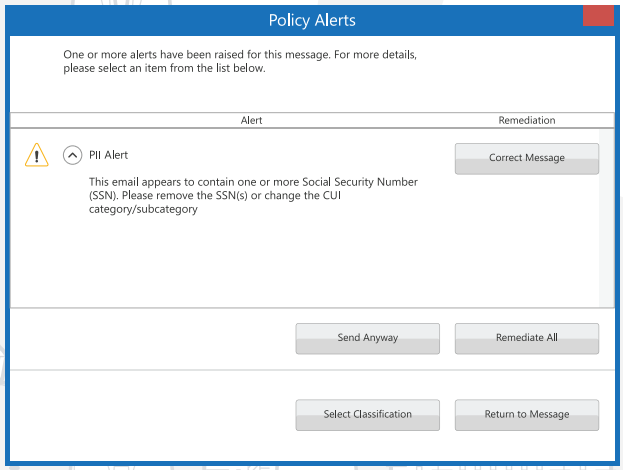
Sensitive information must be identified wherever it sits and however it is created. Titus solutions automatically enforce identification across platforms and devices via easily adoptable workflows to ensure protection of all your information.

Classify

The powerful Titus policy engine ensures that data is classified correctly according to your information security policy. Multiple layers of classification allow for highly granular control.

Deep learning AI technology can be deployed to assess your information, recognise sensitive data and autonomously determine appropriate categories.





Protect

Titus integrates with the other technologies in your security ecosystem, such as messaging, data loss prevention (DLP) and electronic data rights management (EDRM) solutions to enforce your information security policies using open, persistent metadata embedded in documents at creation or upon discovery.

Business leaders can give employees more freedom to innovate and have peace of mind knowing that sensitive information is safe.

Titus supports compliance with cybersecurity regulations by using information security controls that complement your existing security infrastructure, ensuring protection of commercially sensitive and personal data throughout your organisation and wider ecosystem.

The Titus platform is open by design, integrating seamlessly with your existing security stack. As your partner in deploying your security strategy, Titus implements our proven methodology built with over 10 years of experience in data identification and security. Our solution set is designed to support compliance with the NCA ECC-1:2018 for cybersecurity.

1. Governance

1.3 Policies and procedures. Your policy defines the value of your information. Titus helps you build a powerful, flexible framework, customised to your organisation and the information you use.

1.8 Review and audit. Titus supports audits by logging users' data classification compliance. Audit logs will support incident management processes and notification to the authorities if necessary.

1.9 Human resources. As users change roles and eventually leave the organisation, their access control must follow their status. Titus allows multiple classifications to strengthen user access rights.

1.10 Awareness and training. Security is a continuous process. Titus suggests classifications by understanding the context of information, thereby continuously training users to recognise its value.

2. Defence

2.1 Asset management. Titus will intelligently identify and classify data files as they are created or when they enter your organisation. They can be permanently labelled with metadata and physical watermarks.

2.2 Identity and access. Access to information should be restricted to individuals who need to know or use, general least-privileged access or segregated by users' job duties. Multiple open classifications enable strong control.

2.4 Email protection. Incoming and outgoing email must be protected. All emails are scanned for sensitive data, and users are alerted to issues when necessary.

2.6 Mobile devices. Mobile devices and bring-your-own-device (BYOD) programs must be controlled according to job requirements. Titus identification and classification will protect users and data from information disclosure.

2.7 Data and information protection. Information is protected across the organisation's security systems — DLP, EDRM, archiving, etc. — by classification labelling with open metadata.

2.8 Cryptography. Data encryption must be enforced as required. Security systems are directed by Titus classifications to encrypt data at rest and in transit.

2.9 Backup and recovery. Your backup and recovery systems must treat confidential data according to your policies. Titus classifications and metadata trigger these technologies to take the correct precautions to protect information assets.

2.12 Event logs and monitoring. Stay aware of current and developing threats. Titus can log activity and scan for unusual behaviour, such as repeated down-classifying or downloads at unexpected times.

2.14 Physical security. Information should be protected regardless of the device it is on and throughout its life cycle. Titus embedded persistent metadata helps protect data against threats at creation, during storage or after its end of life.

3. Business continuity

3.1 Resilience. Cybersecurity resilience must be maintained across business continuity systems. Titus classifications will direct these systems to apply the correct security protections.

4. Third-party organisations and cloud computing

4.1 Third-party organisations. Third-parties must protect your confidential data. Titus open classifications will direct their systems to protect your data according to your security policies.

4.2 Cloud and hosting. Data held with cloud and hosting service providers should be classified prior to transfer. Titus does this for all information and data files.

5. Industrial control systems

5.1 Industrial control system (ICS) security. Data must be protected across physical and virtual networks. Titus will identify and classify information as ICS data to ensure its safeguarding within the ICS physical and virtual network.

titus
by HelpSystems
www.titus.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.

(tt-sb-0722-db)