With the growth of mobile and cloud technologies, it is more important than ever to secure sensitive information. A lost or stolen mobile device can expose sensitive information or intellectual property. While lost data is a concern to every organization, it has even greater repercussions in regulated industries such as healthcare, finance and aerospace where unintentional disclosure of sensitive information can lead to lawsuits, large fines, damaged reputation or loss of customers.

As Bring Your Own Device (BYOD) and the use of mobile phones and tablets explodes, employees are accessing and storing more and more corporate data on mobile devices. Ideally, organizations would like employees to have access to any sensitive information while in the office, but have this information automatically removed from mobile devices when the employee leaves the workplace.

The use of cellular triangulation and Global Positioning System (GPS) makes it possible for mobile apps to trigger events or actions when the virtual “fence” is crossed. For example, an app could deliver ads specific to nearby local businesses. Since events can be triggered by location, could geofencing be used to automatically delete sensitive email from mobile devices when an employee leaves the workplace?

**Protect Sensitive Information Using Location-Based Services**

Automatically remove sensitive information from mobile devices when employees leave the office

With the growth of mobile and cloud technologies, it is more important than ever to secure sensitive information. A lost or stolen mobile device can expose sensitive information or intellectual property. While lost data is a concern to every organization, it has even greater repercussions in regulated industries such as healthcare, finance and aerospace where unintentional disclosure of sensitive information can lead to lawsuits, large fines, damaged reputation or loss of customers.

As Bring Your Own Device (BYOD) and the use of mobile phones and tablets explodes, employees are accessing and storing more and more corporate data on mobile devices. Ideally, organizations would like employees to have access to any sensitive information while in the office, but have this information automatically removed from mobile devices when the employee leaves the workplace.

The use of cellular triangulation and Global Positioning System (GPS) makes it possible for mobile apps to trigger events or actions when the virtual “fence” is crossed. For example, an app could deliver ads specific to nearby local businesses. Since events can be triggered by location, could geofencing be used to automatically delete sensitive email from mobile devices when an employee leaves the workplace?

**TITUS Mail**

TITUS has developed mobile apps that allow organizations to control the access to and the storage of sensitive email and attachments on mobile devices based on sensitivity and device location. TITUS Mail uses location-based services to help protect sensitive email from leaving the organization.

1. **Protection of Patient Information** – A doctor receives several emails about patient cases on their office iPad. While the iPad is only meant for use while in the hospital, doctors sometimes take their iPad home when they leave. TITUS Mail can detect when the doctor leaves the hospital grounds and can automatically delete all work related email on the mobile device. When the doctor returns to the hospital the TITUS Mail app will once again allow access to work email and the patient’s information.
2. **Financial Services** – A bank employee communicates with a customer about a pending merger and the valuation of the client’s business. The employee uses TITUS Mail to send and receive these emails on their mobile device. When the employee is in the office, they have access to all their email. But when the employee leaves the office, TITUS mail will automatically delete all corporate email from the mobile device. If the phone is lost or stolen, no sensitive customer merger and acquisition information will be at risk. When the employee re-enters the office they can once again access all their email on their mobile device.

3. **Compliance and IP Protection** – An engineer at an aerospace organization has sensitive documents and email about a new jet engine design on his corporate mobile device. This jet engine design falls within the International Traffic in Arms Regulations (ITAR), governing the export and import of defense related material and technologies. The aerospace organization could face multi-million dollar fines if non-US people access this ITAR-protected information. When the employee leaves the borders of the USA on a vacation, TITUS Mail deletes sensitive email and documents from the device. If they lose their mobile device while travelling, no sensitive information will be exposed. When they come back to the US, the employee will once again be allowed to access the engine design information on their mobile device.

### The TITUS Advantage

For over a decade, TITUS has been building solutions to secure sensitive information, and is uniquely positioned to meet the requirements of customers looking to protect information on mobile devices. TITUS Classification for Mobile includes:

- **TITUS Mail** - a secure email app built specifically for organizations that have strict compliance requirements for protecting their sensitive information. Email storage can be controlled based on the device location.

- **TITUS Docs** - a secure container for viewing and sharing files and documents. File sharing can be controlled based on the classification and file type.

TITUS solutions are trusted by over 2 million users in 60 countries around the world. Our customers include Dell, Nokia, Dow Corning, Safran Morpho, United States Air Force, NATO, Pratt and Whitney, Canadian Department of National Defence, Australian Department of Defence, and the U.S. Department of Veterans Affairs.