NOTIFY TECHNOLOGY

Data Loss Prevention

How safe is your corporate data?

SOLUTION BROCHURE

NotifyMDM

Fundamental Elements
- Policies & Security
- Real-Time Statistics
- Location
- App Management
- File Share
- Compliance Manager
- Alerts
- Report Generation
- Logging
- Centralized Monitor
- Self-Service Portal

Supported Devices
- Apple iOS
- Android
- BlackBerry (utilizing NotifySync)
- Windows Mobile
- Windows Phone
- Symbian

Delivery
- On-Premise
- On-Demand (cloud)
- SSAE-16 certified
- 99.9% availability
- Supports VM
- Multi-tenant

Notify Technology
- Providing mobile solutions since 2001
- HQ & Support Center in Canfield, OH
- Highly accessible
- Highly responsive
- Affordable licensing
- Simple, intuitive solutions
- Quality pre and post sales support
- Agile development

Mobile Data Loss Prevention solutions and practices are helping organizations mitigate the loss of confidential company information residing on mobile devices, a particularly sensitive issue among BYOD adopters.

Identifying the Vulnerabilities

What happens when your organizations's confidential, non-public data is left behind on the seat of a taxi or walks to a competitor in the hip pocket of a disgruntled employee? According to Forrester, the most common causes of data breaches are not sophisticated ones rather mundane events such as loss, theft, or unintentional misuse of corporate assets.

Globo solutions can allow users secure access to the data they need while keeping IT in control by using a few best practices.

- Protecting data with end-to-end encryption, device lock, and full or selective wipe
- Protecting access to email, contacts, calendar, and tasks by supporting secure email containerization
- Enforcement of policy compliance through access restrictions and alerts

Having a clear understanding of what is considered confidential data, how it is being used and by who, organizations can better pinpoint the potential gaps where data can be lost. The following considerations can help frame a mobile Data Loss Prevention practice that will avoid or minimize these gaps.

1 Identifying Sensitive Data

- Patient Health Information (PHI)
- Customer Personally Identifiable Information (PII)
- Financial records
- Proprietary & competitive information
- Regulatory Compliance (HIPAA, FINRA, Sarbanes-Oxley)

Identify and prioritize your most valuable data and put in place end-to-end encryption for data in motion and at rest.

2 Considering the Risks

- Email
- Removable storage devices
- Web browsing
- File sharing tools
- Mobile devices
- Network access
- Cloud backup

Consider a secure container approach to email and PIM that controls user actions like save, forward, copy, and paste.

3 Implementation & Deployment

- On-premise or cloud management tools
- Governance of multiple device types and user profiles
- Compliance management to enforce policy
- Security safeguards and procedures for lost/stolen devices

Define policy and get employee consent. Make a technology decision on the tools to help govern and maintain policy.

4 Educating Employees

- Set expectations
- Educate to avoid potential violations
- Promote and reward proper behavior
- Reinforce awareness regularly to deter intentional and malicious breaches

Involve and educate employees so they understand expectations and avoid potential violations.

The Solution: NotifyMDM

NotifyMDM allows organizations real-time visibility and control over smartphones and tablets from a single administrative console. Whether on-premise or in the cloud, NotifyMDM provides a simple, effective, and affordable solution to streamline the deployment and ongoing management and security of smartphones and tablets.