

## University of Guelph

### Company

University of Guelph

### Website

uoguelph.ca

### Industry

Education

### Challenges

Cost-effective method of protecting all data on portable devices.

### WinMagic Solution

WinMagic's SecureDoc SaaS delivery model protects all data stored on servers, desktops, laptops and removable media, such as USB thumb drives and CD/DVDs.

## University of Guelph Selects WinMagic's Cost-Effective SecureDoc™ IT Managed Security/Software-as-a-Service Full-Disk Encryption to Protect All Data on Faculty and Staff Laptop

Wanting to enable its faculty and key administrative staff to take university information home on their laptops to increase overall productivity, University of Guelph (U of G), one of Canada's top comprehensive universities, began looking for a cost-effective method of protecting all data on portable devices.

"An executive Briefing Paper on 'Protection of Sensitive Data' was prepared by our Office of the CIO for our Information Technology Steering Committee (ITSC) in October, 2007," said D. Douglas Badger, CGA CISA CGEIT Director, IT Portfolio Management & Systems Assurance, Office of the CIO, University of Guelph. "This paper emphasized a desire for an 'enterprise approach' to include centralized key management, regulatory compliance and management of the risk of data loss."

With more than 20,000 students and 5,000 faculty and staff, U of G consists of seven colleges whose undergraduate and graduate programs span the natural and physical sciences, social sciences and humanities. Its main campus spans 1,017 acres, including a 408-acre arboretum and a 30-acre research park. Having decided an enterprise-class solution was necessary to protect data on laptops, U of G began mapping out the details.

"In January, 2008 a Whitepaper was prepared by our Manager of IT Security suggesting appropriate enterprise policy on data protection and outlining several technical requirements," explained Badger. "This was followed up by a report to the ITSC in May, 2008, and once this was completed, Michael Ridley, the CIO of the University, tasked my area [Portfolio Management Office/Systems Assurance and Security] with expediting the deployment of an encryption solution," Badger continued. "It was agreed at that time to limit our investigation to vendors offering a cost-effective and easy-to-deploy SaaS (Software-as-a-Service) delivery model."

U of G began looking at SaaS solutions, and having thoroughly researched all alternatives, selected WinMagic's SecureDoc full-disk encryption as the best fit. "Our initial contact with WinMagic led to a visit to their Mississauga head office, and discussions regarding being their 'beta' customer for a SaaS offering of SecureDoc," said Badger. "We were attracted to WinMagic being local to the University, the opportunity to be part of developing the new SaaS service and their responsiveness to our inquiries," Badger continued. "The other vendors we contacted were tardy in responding."

Compatible with Microsoft Windows, Mac and Linux platforms, WinMagic's SecureDoc SaaS protects all data stored on servers, desktops, laptops and removable media, such as USB thumb drives and CD/DVDs. SecureDoc SaaS delivery model ensures that no time is wasted on purchasing, installing and integrating a physical product. SecureDoc's enterprise-class 'always-on' full-disk encryption simplifies the deployment of any combination of sector-based full-disk encryption, file-and-folder encryption, container encryption and self-extractor encryption. This not only makes it easy for organizations to customize data protection to meet specific security protocols, but also 'future-proofs' their investment in encryption. And, in the event that a password is forgotten, or if the user is not available, centralized escrow and management of encryption keys ensure critical data can still be accessed.

**Having selected WinMagic's SecureDoc, U of G began an extensive pilot.**

"As we would be using the SaaS delivery model, integration with existing campus infrastructure was not required, which meant we were able to quickly begin a year-long pilot," commented Badger. "Our initial pilot users were within our IT Security team and Internal Audit department."

**The pilot enabled U of G to iron out any potential deployment complications.**

"We've worked through a few bumps along the way regarding administration," explained Badger. "One complication was our decision to deploy the software to end users through their local IT support technicians," Badger continued. "This entailed creating multiple IDs on each device (administrative and user) and clarification of authorized callers to WinMagic's support desk."

**With the pilot successfully completed, U of G has begun rolling out the new technology.**

"Deployment is voluntary so far with modest promotion, but our target is to secure all portable PCs which store 'sensitive' data," said Badger. "We utilize SecureDoc along with other technologies, such as the Cisco Clean Access Agent for wireless network access control and the STOP program (Security Tracking of Office Property) which our Campus Police department administers."

**The SaaS delivery model has proved a cost-effective, efficient and user-friendly method of protecting all data on portable devices.**

"The SaaS solution is definitely a cost-effective approach at the current volume of encrypted devices, and it has also facilitated very rapid implementation," said Badger. "As mentioned earlier, we adopted the approach of utilizing IT technicians to install the encryption software on behalf of end-users, and so end-user training requirements are minimal," Badger continued. "SecureDoc has proved unobtrusive to the user and feedback has been very positive."

**U of G will now expand its deployment of the SaaS solution as part of its overall data security program.**

"End-point encryption is an important part of a comprehensive security strategy, and we encourage users to be conscious of the risks involved in storing sensitive data on portable devices," explained Badger. "The first statement in our enterprise policy is: 'Sensitive data (including Personally Identifiable Data) should not be stored on portable electronic devices or other electronic media unless absolutely necessary, and approved by department heads,'" Badger continued. "Moving forward, we will expand the deployment of SecureDoc to include all senior management and key administrators."

**WinMagic's SaaS solution has successfully met U of G's data security requirements.**

"We have been very happy with performance of SecureDoc," concluded Badger. "It has met all our data protection requirements without inconveniencing faculty and staff, and I would definitely recommend it to other organizations," Badger continued. "Especially, for resource-constrained IT units who would benefit from the SaaS delivery model."

---

For more information on how WinMagic's SecureDoc can protect your data without interrupting user experience contact Sales@winmagic.com. Visit [WinMagic.com](http://WinMagic.com), or email [info@winmagic.com](mailto:info@winmagic.com)