

Every year more than 200 Schlumberger laptops are stolen or lost. Each loss compromises information security, costs money, and potentially damages our reputation. If your laptop is lost or stolen, depending on the circumstances, it can even affect your wallet. This could also result in disciplinary action; up to and including termination.

### *Top three causes of laptop theft in Schlumberger:*

- 1. Stolen from vehicle**
- 2. Stolen while traveling**
- 3. Stolen from office**



### *Ask yourself the following questions:*

- ◆ Do I need to take a laptop on this trip?
- ◆ Will I use the laptop this evening?
- ◆ Where is the laptop going to be safe?

---

### *Alternatives to your taking laptop :*

---

- ◆ **Access Email from any computer**  
<https://webmail.slb.com>  
Note: You will also have access to Lync
- ◆ **Access SharePoint from any PC**  
Teamspace, My Site
- ◆ **SecureGateway Basic Access from any computer**  
Basic Access: <https://gateway.slb.com>  
Using Secure Gateway Basic Access, you can access the following from your home computer:
  - ◆ Hub , Career Center
  - ◆ Quest, LDAP and LDAP Updates
  - ◆ SABL
  - ◆ Outlook Web Access

---

### *How can I make myself less of a target?*

---

- ◆ Do not display your Schlumberger badge while in transit.
- ◆ When traveling by taxi, do not put the laptop bag in the trunk with your other luggage.
- ◆ Airports and train stations are high risk areas; be aware of the people around you.
- ◆ If you expect to sleep on a trip, ensure your laptop bag is physically next to you where it cannot be disturbed without awaking you.
- ◆ When checking in at the airport or hotel, place your laptop bag on the counter in front of you.
- ◆ If you must place your bag on the floor, loop the strap around one of your legs.

# Schlumberger

## Laptop Loss Prevention



*Schlumberger relies on each and every person with access to information systems to exercise due diligence in the protection of company assets and information. **It's your responsibility to protect your laptop and the information it contains.***

---

## How can I prevent Laptop Loss?

---

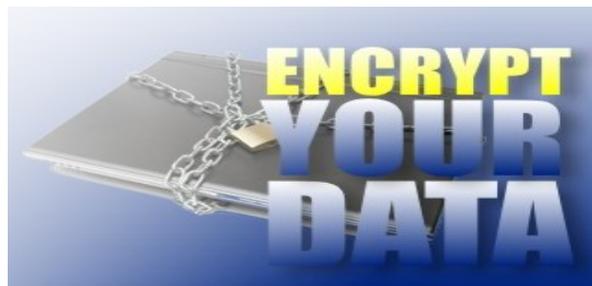
- ◆ **Laptop must be attached with cable lock** to an immobile object while unattended at all times.
  - ◆ **Do not leave your laptop in your vehicle.**
  - ◆ **Keep your laptop under close observation** while traveling.
  - ◆ **Do not check a laptop as baggage** when traveling in an airplane, unless required by local regulations.
  - ◆ **In a hotel room**, lock laptop with a security cable or place it in a locked safe.
  - ◆ **While at home**, keep your laptop in a locked cabinet or secured to an immobile object.
- 

## How to Encrypt your PC?

---

BitLocker is easy to enable and does not impact your computers performance. Ensure your system is backed up before starting the encryption process. Then choose one of the following options:

1. Download and run the package from your SCCM catalog. Click **Start**, select **SCCM** then **Run Advertised Programs**. Download and run "Schlumberger BitLocker 2.x Install".
2. Open a ticket with the Global Service Desk at <http://ithelp.slb.com> or send an email to [ithelp@slb.com](mailto:ithelp@slb.com).



---

## Why Encrypt with BitLocker?

---

- ◆ Protect customer data and company data
- ◆ Protect Schlumberger's reputation
- ◆ Protect personal information and prevent identity theft
- ◆ Avoid contributing to a major or catastrophic RIR
- ◆ Sleep better knowing your confidential data is protected
- ◆ Comply with the Top 12



---

## How to Encrypt Removable Media?

---

It is simple to encrypt removable devices such as USB drives using BitLocker To Go which is included in Windows 7 and 8.x. See [InTouch article #6272944](#).

---

*Be sure to check with your local Site Information Security Coordinator (SISC) for any additional information regarding local security procedures for your location.*

---

---

## What to do if my laptop is stolen?

---

- ◆ File a police report. Obtain a copy of the police report.
  - ◆ Notify the Global Service Desk immediately to change all passwords for corporate accounts.
  - ◆ Notify your direct manager immediately.
  - ◆ Notify your Site Information Security Coordinator (SISC) and ask him/her to help you create an RIR in Quest.
  - ◆ Change all personal passwords.
- 

## Who is responsible for laptop damage / loss??

---

- ◆ Although Schlumberger is responsible for asset damage due to normal daily use, robbery, violence, or forced entry, employees are responsible for asset damage or loss due to employee negligence or non-compliance with security standards.
- ◆ Individuals are responsible for 100% of the replacement cost when loss or damage is due to negligence.

***Don't become a statistic!***

***Take the necessary precautions to secure your laptop at all times.***

