



NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

DRAFT Critical Infrastructure Protection Committee Laptop Computer Theft Avoidance Reference Document

Introduction

The theft of laptop (notebook) computers has been occurring with increasing frequency as the devices have become more common in the workplace. Laptops are very useful for those who work in multiple locations or regularly travel to off-site activities. The NERC Critical Infrastructure Protection Committee (CIPC) recommends the following theft prevention strategies and measures.

Theft Prevention Strategies

1. **Policy** — All electric sector issuers of laptop computers should have a policy which addresses laptop security. The policy should clearly establish expectations for physical and cyber security for the device. This should also include service vehicles equipped with laptop/portable computers.
2. **Consider No Place To Be Safe** — Laptop theft incidents have occurred in virtually every imaginable environment. The laptop computer should be treated as cash and never left unprotected. The device is simply too attractive to a thief.

As an example, Qualcomm's CEO had his laptop stolen while participating in a news conference a mere 30 feet from where he had left it, unattended.

3. **Do Not Advertise It** — Laptop manufacturers (Dell, HP, etc.) make well-designed carrying cases to haul the computers around. Unfortunately, they also put their logos on these cases, letting everyone know what is inside. Considerations should be given to not advertising what is in the piece of luggage.
4. **Be Alert In Public Places** — The prime areas for laptop thefts are busy public places including airports, train stations, public transit locations convention centers, hotels, bars, and restaurants. Laptop thieves like to hang out at places where people may be distracted with other business, such as phone booths, ticket counters, security check in areas, etc.
5. **Vehicle Issues** — Thousands of laptop computers have been stolen from secured vehicles. If left in a visible and identifiable carrying case, it is almost an invitation for a thief to break in and rip it off. If it must be left in a vehicle, always put it out of view in a locked trunk or a covered cargo area. The ability to conceal a laptop should be carefully considered when renting a vehicle. Service vehicles equipped with laptop/portable computers must be kept secure according to each electric sector's policies and procedures.

A New Jersey Nonprofit Corporation

6. **Hotel Security** — Road warriors are aware of the risks of leaving valuables in a hotel room and the same concerns must also apply to laptop computers. If it is necessary to leave the device in a hotel room, consider anchoring it with a security cable to a piece of immovable furniture.
7. **In The Office** — Many laptop thefts occur in the office of the user, especially after normal working hours. When the user leaves for the day, he/she should take the device or lock it away in a desk or cabinet. Keep it secure during the work day by using a lockable docking station.
8. **At Conventions And Conferences** — Laptop thieves like to target these events, especially multiple day events where users tend to become more lax as they become more comfortable in an environment.
9. **Make Laptop Security A Value** — The loss of a laptop is a financial loss and the data lost could be a serious threat. Use common sense in public places, especially when traveling outside one's normal environment. Use a "buddy system" when traveling with friends or associates to help keep an eye on laptops.
10. **Password Security** — It may seem basic in the 21st Century but it's amazing how much data continues to be stored on laptop computers without adequate password protection. A firm, secured password regimen is absolutely required for most laptop computers used in the electric sector.
11. **Higher Level Security** — Many entities in the electric sector are working with higher levels of security for data on laptops. These include multiple password systems, biometric security, voice recognition security, and data encryption.
12. **Asset Tags** — The laptop computer should have permanent markings on the case to identify the device. The U.S. FBI reports 97 percent of unmarked computers are never recovered. Clear permanent and descriptive markings deter casual thieves and assists greatly in any successful recovery.
13. **Register The Laptop With The Manufacturer** — This is an important function when first acquiring a laptop computer. It enables the manufacturer to identify a stolen machine should it be sent in for maintenance. Good record keeping practices must be used to record the serial numbers of all devices.
14. **Security Password Lockout** — Electric sector entities must have procedures to quickly locate stolen laptop computers for access to business or operating systems. A knowledgeable theft could cause significant havoc in systems if not locked out quickly.
15. **Report Thefts To Law Enforcement Rapidly** — Laptop computer recovery after theft is never very high and it deteriorates rapidly as the trail cools off. Law enforcement personnel always encourage thefts to be reported as quickly as possible.
16. **Internal Theft Reporting** — Policies and procedures need to be clearly established and executed to provide complete reporting of any thefts to all appropriate parties within an organization. Each entity needs to establish a clear, quick and easy to initiate notification process.

17. **Software Inventory** — Keeping record of the software loaded on each laptop computer is very important. Recent thefts have been reported where the issuing entity had minimal records of what software was on the stolen machine and what threat the missing computer represented.

18. **Vendors And Contractors** — Electric sector entities often have vendors repair their laptop computers and in some cases, use the computers to execute work for the entity. Any and all policies involving security of laptop computers, the data stored on the computers, and the functionality they provide must apply to vendors and contractors. Contracts with the vendors and contractors need to include specific enforceable language regarding the vendors' obligations to properly secure and protect the devices.