Level 3 Security

LEVEL 3 NETWORK – SURVIVABLE, REDUNDANT, AND SECURE

THE LEVEL 3 APPROACH

With the goal of providing the highest level of security possible, Level 3's business plan includes a comprehensive strategy for protecting the physical and electronic infrastructure of our global network. In fact, our network was built to meet or exceed commercial telecommunications standards worldwide for availability, integrity, and confidentiality.

Our security features are designed to deter, detect, and deny access to unauthorized parties. Continuous network monitoring by our Network Operations Centers (NOCs) allows us to maintain uninterrupted service through immediate detection and remediation. Buried deep, our fiber optic cables are difficult to tap, and our maintenance chambers are fully enclosed reinforced structures. In addition, we constructed our Inline Amplification (ILA) facilities according to stringent security guidelines, and access to our data centers (Gateways) requires passing a minimum of four layers of security.

NETWORK SECURITY

To achieve our network security, we provide:

- Resistant routing
- Tracking systems to trace distributed denial of service and other such attacks to their sources at the edge of the our network
- Collaboration with industry-leading managed security service providers
- Support for legally authorized governmental efforts to trace and identify sources of criminal acts

SECURITY UMBRELLA

For Level 3, "security" is not a single issue. In each arena of our business, we identify risks and threats, and we provide the following countermeasures to protect facilities, equipment, and people:

Level 3 Facilities

- Access controls, customer door locks, closed-circuit television monitoring, and alarms
- Secure access to customer equipment
- Self-contained, industrial-strength power and Heating, Ventilation, and Air Conditioning (HVAC)
- Fire extinguishing system and alarms
- Continuous environmental and security monitoring

Network Systems

- Fail-over systems and continuous monitoring of network
- Access controls, firewalls, and intrusion detection
- Systems security monitoring and recovery
- Secure maintenance chambers and ILA facilities along fiber routes

- Synchronous Optical NETwork (SONET) ring architecture. (In the event of a fiber cut, data in transmission is automatically rerouted to reach its destination via another path.)
- Fiber optic cable shielding and deep burial
- Rapid detection of technical difficulties with fiber optic cables

Personnel

- Adherence to published safety requirements and procedures
- Continuous physical security monitoring
- Rapid response to alarms

LEVEL 3's EXTRA EFFORT

The security staff at Level 3 includes some of the finest in the field. Areas of expertise range from physical security and privacy and data protection to network operation safeguarding. They bolster their knowledge through participation in global governing bodies and organizations devoted to a variety of security issues.

Level 3 is a member of the Association of Certified Planners, Disaster Recovery International, and the Business Continuity Institute. These organizations provide a means for business continuity and disaster recovery professionals to keep abreast of new technology, and to confer with their peers in the industry. Among other shared efforts, these meetings feature speakers from companies that have experienced real disasters and share their "lessons learned."

Also, as a charter member of the Internet Services Provider (ISP) Security Consortium, Level 3 has pledged to work with ISPs on specific detection, prevention, and tracing options that can be deployed industry-wide.

In the area of data privacy, we have met the criteria and recently received "Safe Harbor" status from the U.S. Department of Commerce. Safe Harbor is solely for U.S. companies who receive personal data from European Union Member States, and these U.S. companies volunteer to adhere to seven distinct principles: Notice, Choice, Onward Transfer, Security, Data Integrity, Access, and Enforcement.

Level 3 provides wholesale network services with the highest level of security available, but as a customer, your data security (for example, encryption and authentication) and recovery measures (data backup, off-site storage, and data recovery) are your responsibility. However, we are also committed to providing security assistance beyond the ends of our network. Our help includes tracing problems, addressing sources, and contributing to solutions.

Since the company was founded, we have focused on providing the highest levels of security possible. The success of customers like you is essential for our success, and none of this could be possible without taking measures to ensure physical and electronic security for you and your customers. Good security equals good business.