Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Supplier Security Standard

Purpose

The purpose of this Level 3 Supplier Security Standard is to communicate the minimal logical and physical security requirements for suppliers with access to Level 3 facilities, networks, environments, systems or data and/or when collecting, managing, processing and/or storing Level 3 confidential and proprietary data ("Suppliers").

Scope

The Level 3 Supplier Security Standard is intended for all Suppliers providing services to Level 3.

Overall Program Standard

Supplier shall comply with the Supplier Security Standard during the performance of services for Level 3 and notify Level 3 immediately if an inability to follow the Supplier Security Standard exists. The parties will establish processes and methods of communication so that all documents and information considered sensitive or confidential by either party are securely transported.

The Level 3 Supplier Security Standard also applies to services provided by Supplier's third party vendors, and subcontractors where such services may impact the security of services provided to Level 3. Supplier will create and maintain adequate processes to comply with the Level 3 Supplier Security Standard and will review said processes on a periodic basis to ensure accuracy.

There are basic security requirements that Supplier may need to comply with in addition to the Level 3 Supplier Security Standard. The Level 3 Supplier Security Standard may be revised. Further, the parties agree that, as new technologies for improving security emerge, changes will be made as necessary to help ensure that the Level 3 Supplier Security Standard remains current.

Supplier Personnel (SP)

SP.1 Supplier must have comprehensive HR processes for all personnel that will access Level 3 facilities, networks, environments and/or confidential information or have custody of Level 3 products, assets or confidential data.

SP.2 Upon termination of any Supplier personnel, Supplier must remove access to Supplier facilities and networks for such personnel immediately upon termination, including revocation of access to facilities, account removal to applications, systems and remote access capability. Supplier must also ensure that personnel return all of the Supplier's computers and other assets with access to or containing confidential information, the removal of access to facilities, networks, and/or confidential information. The processes and responsibility for executing these actions must be clearly defined and documented.

SP.3 Supplier must have a security awareness program for all personnel that will access Level 3 facilities, networks, environments and/or confidential information or have custody of Level 3 products, assets or confidential data.

SP.4 Supplier must perform background checks, consistent with Level 3 screening guidelines, for all Supplier personnel seeking access to Level 3 facilities, networks, environments, and/or confidential data, prior to permitting such access. These checks must be done to the extent allowed by local law. See Appendix A for region-specific guidelines.

SP.5 Supplier must provide Level 3 with written certification that Supplier personnel has been favorably vetted in accordance with Level 3 screening guidelines in accordance with SP.4 above; and such personnel is eligible for access to Level 3 facilities, networks, environments, and/or confidential data. Supplier must provide such certification prior to requesting/gaining access to Level 3 facilities, networks, environments, and/or confidential data.

SP.6 All Supplier personnel are required to agree, in writing, to abide by Supplier's physical and information security requirements prior to being granted logical or physical access to Level 3 facilities, networks, environments, and/or confidential data.

Supplier Assessment (SA)

SA.1 Level 3 reserves the right to perform security compliance assessments of Supplier facilities, networks, environments or systems upon reasonable notice and based on the scope of services performed by Supplier. In the event of a security incident, Level 3 may perform immediate audits of the affected facilities, networks and/or environments.

1. "Assessment" could consist of reviews of policies and procedures, technical reviews including vulnerability and software evaluations and requests to obtain evidence of Supplier's control effectiveness.

2. Supplier will be obligated to demonstrate compliance with the Level 3 Supplier Security Standard by providing evidence of deployed control effectiveness. When disclosing such information, both parties will respect Supplier's security policy and existing agreements with other customers regarding Supplier's ability to share information deemed confidential or sensitive.

SA.2 As the result of an Assessment, Level 3 may provide an audit report to Supplier. The audit report will be treated as Level 3 and Supplier confidential information. Within thirty (30) calendar days of receipt of the audit report, the parties will jointly review and agree on the proposed action plan(s) for mutually agreed upon remediation, if any. Supplier will provide Level 3 with periodic updates to the jointly agreed-to action plans until the plans have been fully executed. If an Assessment is rated as unsatisfactory or if Supplier fails to make satisfactory progress with respect to an agreed-to action plan, Level 3 retains the right to conduct an additional Assessment.

Incident Reporting (IR)

IR.1 Supplier must immediately report to Level 3 any security or other event that creates reasonable suspicion of:

1. Unauthorized access to Level 3 facilities, networks, environments, systems or confidential data;

2. Misappropriation or alteration of Level 3 confidential data;

3. Theft, loss of or damage to Level 3 products or assets; and

4. Knowledge of a change in circumstances regarding a formerly screened employee which may cause ineligibility for access.

IR.2 Supplier will take appropriate steps to immediately address any such incident, and will reasonably cooperate with Level 3 with respect to the investigation of such incident. Supplier will promptly provide Level 3 the results of the investigation and will follow Level 3's instructions concerning the security of Level 3's facilities, networks, environments, confidential data, and products/assets. For information security events, e-mail SECOPS@Level3.com

IR.3 Supplier may not make or permit any statements concerning any such incident to any third-party without the explicit written authorization of Level 3's Legal Department.

Supplier Internal Security Requirements (SR)

SR.1 Supplier must maintain a formal written information security policy or policies and procedures for the administration of information security throughout the organization. The information security policy should communicate management's commitment to information protection and the responsibilities of personnel for the protection of information assets.

SR.2 Supplier must apply the following controls to any networks and/or systems that may access Level 3 networks, environments and/or confidential data as well as to any networks and/or systems that contain Level 3 confidential data:

1. Supplier must implement processes and procedures to ensure only favorably vetted and preauthorized Supplier resources have access to the Level 3 facilities, networks, environments, systems and/or data and to the Supplier systems that can access Level 3 systems and/or data or those Supplier systems storing, processing or transmitting Level 3 data.

2. Supplier must immediately disable/remove physical and logical access to Level 3 network infrastructure, systems and/or confidential data for persons, employees, agents, or contractors that no longer have a valid need for access.

3. Supplier must review and update access rights to logical and physical access controls relating to visibility to Level 3 network, systems and/or confidential data or those Supplier systems storing, processing or transmitting Level 3 confidential data at least every 90 days.

4. Supplier must restrict login access to infrastructure to methods that provide individual accountability.

5. Supplier must have roles and responsibilities defined in a manner that allows for segregation of duties and least privilege concept.

6. Supplier must enforce replacement of default passwords, including blank ones, with unique passwords that adhere to Level 3 password policy for any element which has reachability to the Level 3 network, systems and/or confidential data.

7. Supplier must put controls in place to detect and prevent an unlimited number of invalid logon password attempts where supported by the technology.

8. Supplier must ensure relevant security patches are installed with industry standard severity remediation timelines after standard operating environment testing has been completed. If patches are not installed, Supplier must provide evidence of deployed mitigation controls to Level 3.

9. Supplier must maintain all service components at a supported operating system level. Supplier to handle exceptions via Supplier's risk management process including risk identification, remediation plan, and a process to track to completion the upgrade or system decommission. Level 3 must be notified of any parts of Supplier's infrastructure that contains unsupported components.

10. Supplier must use anti-virus software to prevent, detect and remove malicious programs such as viruses, spyware and Trojans.

11. Supplier must deploy technology to scan Supplier's corporate e-mail for viruses and malicious code and keep such technology up to date and within maintenance specifications.

12. Supplier must ensure system logging is enabled where supported by the technology and as dictated by system function. System logs are to be stored for 90 days or other appropriate time period based upon system function.

13. Supplier must register and maintain an inventory of service components that have access to Level 3 facilities, networks, systems and/or confidential data to include information required to adequately respond to security incidents and report on patch and virus signature levels.
    Such an inventory should include at a minimum:
    - System name
    - Supplier personnel assigned to the system;
    - Contact information of the Supplier personnel;
    - Level 3 Supplier project the Supplier personnel is assigned to;
    - IP address or IP address range (if DHCP) of the system;
    - Physical location of the system; and
    - System/Application architecture.

14. Supplier must encrypt all authentication data transmitted over any data network supporting services provided to Level 3 where supported by the technology unless such authentication data is transmitted over a non-inband network, or consists of a one-time password or challenge response password system.

15. Supplier networks used to access Level 3 networks, systems and data or store Level 3 data must have security controls that can protect against unauthorized traffic interception or interference by making use of firewalls, intrusion detection/prevention.

16. Supplier will take reasonably prudent steps to minimize the impact of Denial of Service/Distributed Denial of Service (DoS/DDoS) attacks on devices owned by Supplier. Supplier will ensure procedures are in place to respond in a reasonable and timely manner to such attacks. Supplier will provide 24x7x365 coverage to assist in the mitigation of DoS/DDoS attacks on devices owned by Supplier.
17. Supplier must protect physical locations and equipment that can access the Level 3 network, systems and/or confidential data by preventing and controlling unauthorized access to critical facilities (e.g., network operations centers, switching facilities, data centers, etc.).

18. Supplier must maintain facilities access controls through access management process that includes procedures to add and/or remove people from databases or lists that control access to the Supplier's facilities. Access records shall be kept showing authorizations for access to critical facilities and logs maintained that can identify all who have entered each secured area for at least the prior 90 days.

Access to Level 3 Network (AC)

AC.1 Supplier personnel must sign non-disclosure agreements prior to being given access to the Level 3 network, systems, data or program facilities and provided a security briefing on the program security requirements.

Supplier employees will be required to sign an acknowledgement document indicating that they have received and understand the briefing and the security requirements.

AC.2 Supplier personnel will receive and acknowledge an annual security refresher briefing on additional Level 3 security requirements, if applicable.

AC.3 Supplier will access Level 3's network, systems and associated data only via the Level 3 approved information system resources.

AC.4 Level 3 confidential data will not be transmitted, processed, evaluated or stored outside the Level 3 network environment unless specifically permitted by Level 3.

AC.5 Level 3 reserves the right to implement and maintain security infrastructure that will monitor users' actions while utilizing the Level 3 environment. Any unauthorized activity detected using these security controls will be reported to the Supplier Security POC.

AC.6 Level 3 reserves the right to remove any Supplier resource for violation of the Level 3 Supplier Security Standard. Such removal of a resource may be from current and future Level 3 Supplier projects.

AC.7 At no time will Supplier employees share credentials, badges, passwords or other uniquely identified resources when accessing Level 3 networks, systems and data.

AC.8 The Level 3 LAB environment will operate with the following controls:

- Access to Level 3 network lab environments may involve software and hardware configuration requirements. Supplier partners must notify Level 3 Security when LAB environment access is required for a Supplier service.
- Level 3 may provide time of day/day of week controls for access into the Level 3 lab environment.

AC.9 The Level 3 network will operate with the following security controls:

- Access to Level 3 network may involve special software and hardware configuration requirements. Supplier partners must notify Level 3 Security when management access is required for a Supplier service.
- Software may need to be installed on Supplier systems in order to facilitate access to the network. When such software is required, Level 3 will also require the implementation of security software to monitor the security of the system and its interaction with the Level 3 network.

Protection of Level 3 Data in Supplier's Possession (PD)

PD.1 Level 3 confidential data must not be sent to third party networks without pre-authorization from Level 3 Security Compliance.

PD.2 Level 3 confidential data must not be sent via the Public Internet without pre-authorization from Level 3 Security Compliance.

PD.3 Supplier must report any Level 3 confidential or sensitive data when discovered on unapproved Supplier systems and immediately remove it from unapproved Supplier systems and notify Level 3 of such incident.

PD.4 Level 3 confidential data must be transmitted securely and encrypted when stored utilizing Level 3 approved encryption tools and methodology.

PD.5 Level 3 confidential data authorized for storage on Supplier systems must be protected in accordance with Level 3's data security standard.

PD.6 Level 3 confidential data authorized for storage on Supplier systems must be deleted, via a secure method approved by Level 3 Security, after use or upon termination of Supplier service; whichever occurs first.

PD.7 In the event there is any loss of Level 3 confidential data, or any unauthorized or unlawful access to, use of, or disclosure of, or any other compromise of Level 3 confidential data, Supplier shall immediately notify Level 3 in writing of the security incident. Supplier shall (i) fully cooperate with Level 3 to investigate and resolve the security incident, including without limitation, agreeing to the content of any notifications of the security incident, (ii) be responsible for all costs related to any security incident, including without limitation, costs related to investigations, notifications, customer support and credit monitoring, and (iii) properly document responsive actions taken related to any security incident, including without limitation, post-incident review of events and actions taken, if any, to make changes in business practices related to the protection of Level 3 data, escalation procedures to senior managers, and any reporting to regulatory and law enforcement agencies.

Facility Physical Security (FS)

FS.1 Security controls must protect against theft or unauthorized access to facilities, confidential information, environments, networks and any other technology assets.

FS.2 The facility must have a physical security plan that covers internal and external threats to the site and is reviewed and updated by Supplier's facility management team at least on an annual basis. If requested by Level 3, Supplier must provide the plan to Level 3 for review and approval.

FS.3 The facility must have physically secure perimeters, and external entry points must be suitably protected against unauthorized access. Access to all locations must be limited to Supplier personnel and authorized visitors. Out of hours access must be monitored, recorded and controlled. Logs detailing access must be stored for a period of ninety (90) days to the extent permitted by local law

FS.4 Access to areas where confidential information is stored or accessed must be restricted to authorized personnel. Such areas must be situated away from public areas and access must be restricted using reasonable access controls and authentication mechanisms.

FS.5 All Supplier personnel and authorized visitors must be issued identification cards. Visitor identification cards must be easily distinguishable from Supplier personnel identification cards and must be retrieved daily.

FS.6 Suppliers must monitor and manage the possession of access cards and keys that provide access to service locations and ensure access is limited to authorized personnel only.

FS.7 A clear desk policy must be enforced throughout the Supplier facilities where networks are accessed and/or confidential information is stored or accessed. Documents that contain confidential information must be secured when not in use. Supplier personnel must have access to a secure, locked cabinet in which to store such documents.

FS.8 Supplier personnel must abide by Level 3 site-specific physical security standards when accessing Level 3 facilities.

Related policies, processes and standards

- Supplier Security Policy

Appendix A – Screening Guidelines

US Suppliers must be screened to the Level 3 standard:

- Previous employment verification for at least the past seven (7) years, including military records as applicable;
- Social Security verification
- Criminal records check for the past seven years
- Verification of professional licenses as applicable
- Department of Motor Vehicles check as applicable.

UK Suppliers must be screened to the Baseline Personnel Security Standard (BPSS), which includes verification of:

- Identity
- Nationality and Immigration Status (including an entitlement to undertake the work in question)
- Employment history (past 3 years)
- Criminal record (unspent convictions only)
- Additionally, prospective employees are required to give a reasonable account of any significant periods (6 months or more in the past 3 years) of time spent abroad.

All other countries, suppliers must be screened to the extent legally allowed, for the following:

- Identity
- Right to work
- Employment history
- Criminal record