



# Level 3 Communications Vendor Services Security Model

<b>DOCUMENT NUMBER:</b>	L3NSD:VendorSecurity:061709:01
<b>ISSUE:</b>	4.0
<b>CURRENT RELEASE DATE:</b>	8/10/11
<b>AUTHOR :</b>	Level 3 Security Architecture
<b>OWNER:</b>	Level 3 Communications
<b>AUTHORIZER :</b>	Dale Drew, Chief Security Officer

## **Preface**

Nothing herein is to be construed as a warranty or guarantee, expressed or implied, regarding the performance, merchantability, fitness or any other matter with respect to the products, nor as a recommendation to use any product or process in conflict with any patent.

This document provides high-level security requirements associated with partners whom need to gain access to Level 3 networks, systems and data relating to Level 3 outsourcing projects.

The threats to information assets are continually changing, and readers are encouraged to contact:

Level 3 Global Security Department - DL-PolicyGroup@level3.com for any questions or clarification of the issues addressed herein.

## **Exception**

These security considerations have been analyzed to provide as much implementation practicality as possible, from both an engineering and operations perspective. The solution(s) raised within this document are meant to be a secure, scalable, reliable, and cost-effective method of meeting the design challenges of protecting corporate products, resources and systems to meet Level 3's standards of integrity, confidentiality and availability.

Level 3 Global Security Compliance must approve any request for an exception to these design considerations:

DL-PolicyGroup@level3.com.

## **Important:**

This publication may not be reproduced, stored in a retrieval system, or transmitted in whole or part, in any form or by any means electronic, mechanical, audio, photocopying, recording, or otherwise outside of the acceptable use of the Level 3 confidentiality markings policy.

---

# ***1. Introduction***

## **1.1 Purpose**

The purpose of this document is to communicate the minimal logical and physical security requirements for vendors when connecting into the Level 3 internal networks and when collecting, managing, processing and/or storing Level 3 confidential and proprietary data.

Vendor will be required to be compliant with these Security Requirements when providing services to Level 3. Level 3 will reserve the right to audit and validate that the Security Requirements are being followed and are maintained as part of an implemented and consistent process.

## **1.2 Intended Audience**

This document is intended for Level 3 vendor partners whom are providing vendor services to Level 3.

## **1.3 Revision History**

The table below chronicles the revision history of this document.

<b>Revision</b>	<b>Date</b>	<b>Author(s)</b>	<b>Reason for Change</b>
1.0	3/29/07	D. Drew	First Draft Release
2.0	6/8/08	D. Drew	Peer review comments
3.0	6/8/09	D. Drew	Peer review comments
4.0	8/10/11	Natalia Issatchenko	Updates

## **1.4 Document Security**

This document contains information classified **Level 3 Confidential**

---

## ***2.0 Vendor Security Requirements***

### **2.1 Overall Policy Issues**

1. Vendor shall comply with Level 3 Logical and Physical Security Company policies, procedures and standards, hereafter called "Security Policy". Vendor shall be provided access to updates of the Security Policy when a critical security policy is introduced, during the life of the contract. Vendor shall acknowledge the Security Policy upon receipt and indicate if an inability to follow the Security Policy exists.
2. Vendor shall minimally implement security controls for the Service(s) that are governed by the Security Requirements document as described herein.
3. Level 3 expects Vendor to manage Security Requirements related to Services provided by Vendor's third party vendors, and subcontractors where such Services may impact the security of Services provided to Level 3. Vendor will create and maintain adequate processes to implement these Security Requirements and will review said processes on periodic basis to ensure accuracy.
4. As applicable to Services, and based upon a jointly agreed-to process, Vendor will provide an initial review of its then current security policy to Level 3 that implements the Security Requirements from this document. At no additional charge to Level 3, subsequent to the initial review, Vendor shall allow Level 3 to review the Vendor's current Security Policy on periodic basis. For security policy updates, Vendor will supply Level 3 with a summary of any changes. Vendor's Security Policy shall be considered Proprietary Information and shall not be distributed within Level 3 to employees who do not have a need to know.
5. The parties agree that any additional Security Requirements identified by either party as necessary for additional Services or new services, will be added to the this document and will be mutually agreed upon. Further, the parties agree that, as new technologies for improving security emerge, this document will be amended as necessary to help ensure that the Security Requirements remain current.

6. 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.
7. Vendor will conduct periodic security reviews with Level 3 with meeting minutes recorded and archived for 1 year.
8. Vendor shall provide a Security Point of Contact relating to the execution and maintainance of the Security Requirements. The Security Contact should be able to be an authority to Level 3 for at least the following areas:
  - Physical Security Controls
  - Logical Security Controls
  - Quarterly Update Meetings
  - Policy and Procedures within the Vendor
  - Incident Response
9. Level 3 reserves the right to filter, restrict, block any traffic, user or service originating from the Vendor network to Level 3 for any reason, at any time without prior notice.
10. Any exceptions to the Security Requirements will need to be approved in writing by the Level 3 Security Compliance Department
11. Vendor employees, Vendors or contractors prior to being given unescorted access to Level3 systems, data or program facilities will be provided a security briefing by the Vendor on the program security plan requirements. Vendor employees will be required to sign an acknowledgement document indicating that they have received and understand the briefing and the Security Requirements document.
12. Vendor employees, vendors or contractors will sign program non-disclosure agreements prior to being given access to Level3 systems, data or program facilities.
13. Vendor employees will receive and acknowledge an annual security refresher briefing on program security requirements.

## **2.2 Access to Level 3 network, systems and data**

1. Vendor will access Level 3's network, systems and associated data only via the Level approved resources.
2. Level 3 confidential data will not be transmitted, processed, evaluated or stored outside the Level 3 network environment unless specifically permitted.
3. Level 3 reserves the right to implement and maintain security infrastructure that monitors users actions while utilizing the Level 3 environment. Any unauthorized activity detected using these security controls will be reported to the Vendor Security POC.
4. Level 3 reserves the right to remove any Vendor resource for violation of the Security Requirements. Such notifications can include immediate removal of a resource from current and future Level 3 Vendor projects.
5. At no time will Vendor employees share credentials, badges, passwords or other uniquely identified resources when accessing Level 3 systems and data.
6. 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. Vendor partners must notify Level 3 Security when LAB environment access is required for a Vendor Service.
  - Level 3 may provide time of day/day of week controls for access into the Level 3 lab environment.
7. The Level 3 Management environment will operate with the following security controls:
  - Access to Level 3 management network may involve special software and hardware configuration requirements. Vendor partners must notify Level 3 Security when management access is required for a Vendor Service.
  - Software may need to be installed on Vendor systems in order to facilitate access to the management 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.

### **2.3 User Access to Systems**

1. Access to Level 3 systems must be submitted by a Level 3 Vendor project coordinator through the standard 3Help process.
2. Access to systems must be done via the use of Level 3 multi-factor authentication whenever the allowed by the system.
3. Vendor users must not share Level 3 assigned access credentials to Level 3 systems.
4. Vendor users must not access Level 3 systems or resources that they have not been explicitly provided permission to access.

## **2.4 Protection of Level 3 Confidential Data**

1. Level 3 Confidential or Sensitive Data must not be sent to third party networks without pre-authorization from Level 3 Security Compliance.
2. Level 3 Confidential or Sensitive Data must not be sent via the Public Internet without pre-authorization from Level 3 Security Compliance.
3. Vendor will report any Level 3 Confidential or Sensitive Data when discovered on unapproved vendor systems and immediately remove it from unapproved vendor systems.
4. Any Level 3 data must be transmitted securely and encrypted when stored utilizing approved by Level 3 encryption tools and methodology.
5. Any Level 3 Confidential or Sensitive Data authorized for storage on vendor systems must be protected in accordance with Level 3 Security Policy.
6. Any Level 3 Confidential or Sensitive Data authorized for storage on vendor systems must be deleted, via a secure method approved by Level 3 Security Compliance, after use or upon termination of Vendor Service; whichever occurs first.
7. In the event there is any loss of Level 3 Sensitive or Confidential Data, or any unauthorized or unlawful access to, use of, or disclosure of, or any other compromise of Level 3 Sensitive or Confidential Data, Vendor shall immediately notify Level 3 in writing of the Security Incident. Vendor 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 Sensitive or Confidential Data, escalation procedures to senior managers, and any reporting to regulatory and law enforcement agencies.

8. Any exceptions to the above controls will need to be approved in writing by the Level 3 Security Compliance Department.

## **2.5 Incident Reporting**

1. The parties will cooperate in the immediate containment and investigation of Service-related security incidents that impact Level 3 or Authorized Users. The party first learning of such an incident shall promptly inform the other of any actual or suspected security breaches, including unauthorized network intrusions. The parties will assign points of contact, which may be updated from time to time, for Service-related security incidents.
2. Vendor will inform Level 3 Security Operations Center of incidents when Vendor determines that Level 3 or Level 3's Authorized User's data, or a Service has been compromised, and will engage in joint investigative activity if needed. To the extent feasible and as permitted by applicable law, detailed information (including but not limited to IP address, origin, offending and/or compromised userid, and logs or reports that would assist Level 3 with their forensic investigation) will be shared among the parties' investigative units on a need to know basis. Vendor will record and report on security incidents and issues and report to Level 3 any network security incidents affecting the Service to Level 3 or Level 3's Authorized User. Such records shall be retained in accordance with Vendor's document retention policies. In the event of a network security breach, Level 3 can obtain daily updates. The parties will mutually define and agree upon an incident management plan.

## **2.6 Security Of Vendors Network**

1. Level 3's corporate security has adopted the ISO 27002 and NIST 800-53 frameworks as an internal baseline measurement of security posture. Level 3 is using a self-assessment process as a supplement to a global

controls assessment process and as a means of assessing the security posture of all vendors or potential business partners.

2. Vendor must maintain a secure logical and physical environment to ensure the highest levels of integrity when accessing Level 3 systems and data. Vendor will communicate to Level 3 its Security Policy, Standards and Methodology for implementing security and will provide to Level 3 updates when such policy is modified.
3. Vendor deploys technology to scan Vendor's corporate e-mail for viruses and malicious code and keeps such technology up to date and within maintenance.
4. Vendor will 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 systems and/or data.
5. Vendor will put controls in place to detect and prevent an unlimited number of invalid logon password attempts where supported by the technology.
6. Vendor will implement processes and procedures to ensure only preauthorized Vendor resources have access to the Level 3 systems and/or data and to the Vendor systems that can access Level 3 systems and/or data or those Vendor systems storing, processing or transmitting Level 3 Confidential or Sensitive data..
7. If Vendor makes a determination that a valid need for access to Level 3 systems and/or data no longer exists, within 24 hrs disable/remove physical and logical access to network infrastructure, systems, and components for persons, employees, agents, or contractors that no longer have a valid need for access.
8. Vendor will review and update access rights at least every 30 days to logical and physical access controls relating to visibility to Level 3 systems and/or data network or those Vendor systems storing, processing or transmitting Level 3 Confidential or Sensitive data.
9. Vendor will take reasonably prudent steps to minimize the impact of Denial of Service/Distributed Denial of Service (DoS/DDoS) attacks on devices owned by Vendor.. Ensure procedures are in place to respond in a reasonable and timely manner to such attacks. Provide 24x7x365 coverage to assist in the mitigation of DoS/DDoS attacks on devices owned by Vendor.
10. To the extent feasible and as permitted by applicable law, work with Level 3 during a material network attack investigation in tracing the origin of packets that appear to be originating from inside the Vendor network.

11. Ensure relevant security patches are installed according to Level 3's specified time limits after standard operating environment testing has been completed. In cases, where patches are not installed, Vendor must provide evidence of deployed mitigation controls to Level 3.
12. Maintain a primary and backup subscription process that enables Vendor to be informed of any new security advisories issued by network infrastructure vendors and an industry standard advisory service (e.g. CERT). Obtain security patches from reputable sources (e.g. equipment suppliers).
13. Maintain all Service Components at a supported operating system level. Vendor to handle exceptions via Vendor'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 Vendor's infrastructure that contains unsupported components.
14. 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.
15. Register and maintain an inventory of Service Components that have access to Level 3 systems and/or data to include information required to adequately respond to security incidents and report on patch and virus signature levels. Such an inventory should include:
  - System name
  - Vendor employee assigned to the system
  - Contact information of the Vendor employee
  - Level 3 Vendor project the Vendor employee is assigned to
  - IP address or IP address range (if DHCP) of the system
  - Physical Location of the system
16. Take corrective action dealing with identified security violations of Vendor customers on Vendor networks that materially impact Level 3 including shutting down connectivity into Vendor and or Level 3 environment (where possible) if so formally requested by Level 3.
17. Manage Vendor TCP/IP network infrastructure security and administrative users in support of Services according to Vendor's Security Policy which must at a minimum include the following requirements:
  - Restrict login access to managed network infrastructure to methods that provide individual accountability;

- If a determination is made that a valid need for access no longer exists, disable/remove logical access to network infrastructure, systems, and components for persons, employees, agents, or contractors that no longer have a valid need for access within 24 hours of that determination; and
  - Every three months, review access lists for network infrastructure security and administrative userids and update as required to ensure accuracy. Records of updates shall normally be kept and maintained for at least 180 days.
18. The Vendor 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.
  19. Log successful or unsuccessful administrative or management access attempts, including SNMP and all console access, to Vendor managed Service Components, where supported by the technology and as dictated by system function.
  20. Regarding IP-related Services, have reasonably adequate response mechanisms (i.e. closing ports) in place to address traffic that is deemed as malicious or hostile. With respect to Level 3's Vendor Services, Vendor will work in good faith with Level 3 to implement response mechanisms to address Level 3's reasonable concerns relating to malicious or hostile traffic.
  21. Any Service Component capable of displaying a warning screen message must display a business use notification at the first point of log on.
  22. Protect the physical security of locations and equipment in which access to the Level 3 network is routed or where Vendor systems that can access the Level 3 systems and/or data are located by preventing and controlling unauthorized access to critical facilities (e.g., network operations centers, switching facilities, data centers, etc.).
  23. Facilities access controls shall be maintained through an identification process that includes procedures to add and/or remove people from databases or lists that control access to the Vendor'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.

## **2.7 Right to Audit**

1. On thirty (30) calendar days prior written notice, Level 3 may conduct an “Review” in order to determine Vendor’s compliance with the Level 3 Security Requirements and Vendor’s related security processes by reviewing evidence of their implementation. “Reviews” could consist of reviews of policies and procedures, technical reviews including vulnerability and software evaluations and requests to obtain evidence of Vendor’s control effectiveness. Vendor will demonstrate compliance with this Security Requirements Document while both parties still respect Vendor’s security policy and existing agreements with other Vendor customers regarding Vendor’s ability to share information deemed confidential or sensitive. Vendor agrees to discuss findings, if any, discovered by Level 3 during the Review and to implement such remediation activities as the Parties mutually agree are necessary.
2. Within thirty (30) calendar days of receipt of Review findings, the parties will jointly review and agree on the proposed action plan(s) for mutually agreed upon remediation, if any. Vendor will provide Level 3 with periodic updates to the jointly agreed-to action plans until the plans have been executed. If a Review is rated as unsatisfactory, Level 3 retains the right to conduct an additional Review within the Contract Year.
3. For avoidance of doubt, all information that is shared with Level 3 shall be deemed “Confidential Information” and shall be treated in accordance with the Confidential Information provisions of the Agreement.