CenturyLink Service Guide

Incident Management and Response

This CenturyLink Service Guide ("SG") sets forth a description of the Incident Management and Response ("Service") offerings by CenturyLink, including technical details and additional requirements, if any. This SG is subject to and incorporated into the Service Agreement and Security Service Schedule between the parties. The specific details of the Service ordered by Customer will be set forth on the relevant Service Order. For avoidance of doubt, any references in the Agreement, Schedules, or Service Orders to SSG, shall mean SG.

Version	Previous	Section Modified	Date
SEC-SG-INCIDENT MANAGEMENT AND RESPONSE _110816	N/A	All	11/08/16

Table of Contents

Service Description

Incident Management and Response

1. **Service Description**: The Incident Management and Response service ("Service") is an optional add-on service to the Security Log Monitoring ("SLM") service ("SLM Service"). SLM Service must be purchased by the Customer before Incident Management and Response Service may be purchased. SLM Service provides the identification and notification of a security event to a Customer, with no further action by CenturyLink. With Incident Management and Response Service, when an incident is identified, CenturyLink will assign an Incident Coordinator who will escalate and coordinate with the Customer the steps needed to allow the Customer to assess incidents and contain or eradicate the issue. The Incident Coordinator will work with the Customer in a project manager role as detailed below, to assist Customer with its normalization of the affected service. This Service is intended to provide an additional layer of incident management support for the Customer, with the actual containment, eradication, and recovery work to be performed by the Customer. No SLA applies to this Service.

2. **Service Components**

2.1 Client Incident Management Plan Assessment: An analysis of the client's current incident management plan must be conducted by CenturyLink before this Service can be enabled. The analysis is intended to evaluate whether the Customer's existing incident management plan is prepared to effectively respond to information security incidents when they occur. Customer will allow for a minimum of 2 weeks for CenturyLink to review. If Customer does not have an existing incident management plan, then CenturyLink will provide a standard plan template as a baseline starting point. Following the evaluation, CenturyLink and Customer must then mutually agree in writing the Incident management plan to be used for the Service ("Client Incident Management Plan"). The Client Incident Management Plan will include, but not be limited to, mutually agreed personnel resource requirements of Customer and CenturyLink. Throughout the Service Term, the parties may agree to modify the Client Incident Management Plan however Incidents will follow the version of the plan in place when the Incident is identified.

2.2 Incident Identification: For the purpose of this Service Guide, an "Incident" is defined as: "A verified event or set of events, that has resulted in a negative change to the availability, integrity, or confidentiality of Customer information, technology, or other data contained within."

Identification of an Incident occurs within the SLM Service, which analyzes all incoming events to confirm the basic nature of the event and rule out false positives. Each event is "verified" because until it has been accurately determined that such an event has occurred, the complete Incident response process under this Service Guide will not be pursued. If the event is verified as an Incident, then CenturyLink and Customer, using the agreed Client Incident Management Plan, will commence the steps described below (collectively, the "Incident Response Process").

2.3 Incident Response Process

2.3.1 Phase 1 - Assessment: The assessment phase begins under the SLM Service where the core activity of the Incident Response Process occurs. In this phase, once an Incident has been identified by SLM Service, the issue is escalated to the CenturyLink Iincident Management Response organization, a response team will be formed, and the investigation will be conducted with the primary goals of identifying the scope of the Incident and determining the technical aspects of the Incident necessary to inform the Customer of its options for containment and eradication.

2.3.1.1 Severity Determination: The severity of a given Incident determines the level of response and the speed of response activities as mutually agreed by Customer and CenturyLink in

the Client Incident Management Plan. Severity will be determined using the Microsoft DREAD model, which can be found at the following link:

http://msdn.microsoft.com/en-us/library/ff648644.aspx

DREAD Rating Categories
The DREAD model scores risks by rating each Incident within several different categories, and then combining the score.

Probability Ratings:

- Discoverability: How easy is it to discover elements of the Incident?
- Reproducibility: How easy would it be to reproduce a successful exploitation of the Incident?
- Exploitability: How difficult is it to exploit the Incident?

Impact Ratings:

- Affected Users: How many people (Employees, customers, etc.) will be impacted?
- Damage: How severe is the damage likely to be?

Scoring
The Incident Coordinator assigns an Incident a score from 0-10 within each of the categories above, with 0 being the lowest score or probability rating, and 10 being the highest. Once the Incident is scored in all five categories the scores are combined, and the Incident is assigned according to the following table:

Total Score	Risk Rating
80-100	Critical
60-80	High
30-60	Medium
0-30	Low

2.3.1.2 Incident Response Pathway based on Severity Level:

There are two primary Incident response pathways, and in each case Incident response teams will be engaged by severity type as mutually agreed in the Client Incident Management Plan:

Express Incident Response – is a lower activity process to deal with LOW severity threats and vulnerabilities as defined by the DREAD model above.

Full Incident Response – is a higher activity process that deals with MEDIUM, HIGH, and CRITICAL Incidents.

2.3.2 **Phase 2 - Containment and Eradication:** In the containment and eradication phase, CenturyLink will advise Customer of options that Customer may pursue to prevent the increase of the scope of the Incident, and to limit the possibility of additional unauthorized activity on assets that have already been affected. The level of severity of the threat will determine how quickly CenturyLink will provide its initial recommendations, but typically this may be as little as several hours for Critical Incidents and up to five (5) days for Low severity Incidents.

Customer is ultimately responsible for deciding how it will contain and eradicate an Incident, as well as for performing the tasks necessary for such containment and eradication. CenturyLink's role is to compile information, suggest options, and assist Customer with its project management of the Incident.

2.3.3 **Phase 3 - Recovery:** The purpose of the recovery phase is to return affected assets to a state that includes full operational status but at reduced risk of a duplicate event occurring.

The success of the recovery phase is greatly dependent on Customer's pre-established event process mutually agreed in the Client Incident Management Plan, and may include CenturyLink coordination or project management. The Customer's security response team must:

- Restore the affected systems to normal operation
- Restore from backup tapes, or rebuild systems
- Correct vulnerabilities found and conduct tests to verify that systems are no longer vulnerable to a similar incident.
- Shutdown / remove completely old server(s) from the environment
- Test for overall functionality

Upon Customer's request, CenturyLink will include documented details in CenturyLink's standard post-mortem / root-cause analysis report.

2.3.4 **Phase 4 - Follow-Up:** The purpose of the follow-up phase is to confirm that the end state conditions have been met (per Table 1.0), and that reports have been written and provided as requested and agreed by the parties. For the purposes of this SG, end state means that Customer has taken required actions and the Incident has been contained and/or eradicated.

All previous phases are reviewed and evaluated for possible improvements that could be made to Customer's previously agreed Client Incident Management Plan, Customer's policies, procedures, and/or system configurations.

2.3.5 **Phase 5 - Incident Closure**: The following table (Table 1.0) represents the end state conditions that must be present in order for this phase to be completed. Subject to Section 4.5 below, when Customer informs CenturyLink that these conditions are met, the Incident Coordinator will close the Incident.

Table 1.0 End State Conditions for Incident Closure

CenturyLink Assessment Team	Customer Core Management Team	Customer Extended Management Team (as needed)
All search / detection measures complete with no new findings.	Assessment Team reports complete.	Core Management Team reports complete.
Examination tasks have been completed.	Satisfied with answers to all investigative questions.	Satisfied with answers to all investigative questions.
Investigative questions have been answered or determined unanswerable.	No new questions.	No new questions.
➔	➔	

3. **CenturyLink Response Team**: The following CenturyLink roles may participate as mutually agreed in the Client Incident Management Plan, depending upon the severity determination of an Incident:
    - Incident Coordinator: As the primary technical manager of an information security incident response effort, the Incident Coordinator will lead the Core Management Team.
    - Incident Project Manager: A project manager is designated to assist with the response and responsibilities including providing structure and discipline to associated activities.
    - Regional Security Lead: The Regional Security Lead for each customer region affected will sit on this team to serve as the technical security expert for the information systems in those regions.

4. **Customer Responsibilities**:
    - 4.1. Customer acknowledges the Service is offered as one tool to be used as part of an overall security strategy, and not as a total security solution.
    - 4.2. Customer must ensure the specific Customer response team members, as mutually agreed in the Client Incident Management Plan, are available to CenturyLink as needed for the Services on CenturyLink's request.
    - 4.3. Customer is solely responsible for any mitigation activities, including the containment and eradication of Incidents, needed changes to prevent recurring Incidents, and any and all system or network changes.
    - 4.4. Customer acknowledges and agrees CenturyLink's role for the Services herein is solely collaborative and advisory.
    - 4.5. Customer is responsible for notifying CenturyLink within 10 business days of the date CenturyLink provided its initial recommendations for containment and eradication (as described in Section 2.3.2

above) that the end state conditions for Incident closure have been met, and no response from Customer is deemed to mean end state conditions were met. Notwithstanding the foregoing, if the suggestion(s) for containment and eradication initially provided by CenturyLink were not effective even after all recommended actions were taken by the Customer, Customer may, prior to the required 10 business days' notice above, request that the parties' response teams review the available information generated throughout the Incident Response Process to determine any other recommendations. After such review, CenturyLink will provide Customer with a written notice that will either include a second set of recommendations or state that CenturyLink was unable to determine any new recommendations. 5 days after the date of such notice, whether or not the Incident is contained and eradicated, the Incident Coordinator will close the ticket. If an Incident reoccurs after closure, a new Incident ticket will be generated. In no event will CenturyLink be required to provide more than 2 sets of recommendations per Incident.

5. **Roles and responsibilities**: for both CenturyLink and the Customer are marked with an "X" in the appropriate column in Table 2.0 Standard Roles and Responsibilities.

Table 2.0 Standard Roles and Responsibilities

Phase	Task	CenturyLink	Customer
Incident Management Plan Assessment:	Analyze Customer plan and provide guidance	**X**	
	CenturyLink to provide standard plan template if none available from Customer, then the parties must mutually agree the plan before proceeding	**X**	**X**
Identification	Occurs as part of the SLM Service	**X**	
Assessment	CenturyLink response team conducts investigation	**X**	
	The severity determination of the incident is made by CenturyLink utilizing DREAD model and notifies customer	**X**	
	Customer response team notified and conducts investigation		**X**
Contain and Eradicate	Per the agreed Client Incident Management Plan, CenturyLink will work with the Customer to advise on possible action plans.	**X**	
	Customer is responsible for the containment and eradication of Incidents.		**X**
Recovery	CenturyLink will coordinate and work with Customer's Incident response team in an advisory role.	**X**	
	Customer responsible for recovery activities needed to bring service back to normal operation.		**X**
	Upon Customer's request, CenturyLink will provide CenturyLink standard root-cause analysis reporting.	**X**	
Follow-Up	Once end state conditions have been met, CenturyLink to review Incident and response and advise Customer on optional adjustments to Customer's Client Incident Management Plan, policies, and/or system configurations.	**X**	
	Customer evaluates and may decide to adjust its Incident response plan, policies, and/or system configurations.		**X**
Incident Closure	Once the end state conditions have been met per Table 1.0, and the follow-up phase has been completed, the Incident will be closed.	**X**	

6. Billing:

CenturyLink will bill Customer monthly in advance for the base Incident Management and Response Service monthly recurring charges ("MRCs") as defined in the applicable Service Order associated with the Service. For Incidents above the base amount, there is an additional per Incident usage charge billed in arrears. CenturyLink uses the total Incidents over one month to calculate the additional Incidents usage charges above the base MRCs.

For example, if Customer purchased 3 Incidents per month for an MRC of $1000 with a variable usage charge of $500/Incident, and actual usage over the month was 4 incidents, then Customer would be billed the $1,000 MRC for the 3 Incidents, and a usage charge for the additional 1 Incident of $500 on the next month's bill.

7. Service Limitations:

7.1. Notwithstanding any other provision or understanding to the contrary in any document, CenturyLink makes no representation, warranty, or guarantee that the Service will be uninterrupted or error-free; will detect or generate an alert for every security event that may be recorded in customer logs; or that any of the tasks performed hereunder comply with or satisfy any applicable governmental or industry data security standard. Customer acknowledges that CenturyLink may not identify all possible incidents or vulnerabilities and CenturyLink expressly disclaims any responsibility for any unidentified or misidentified incidents or vulnerabilities. If CenturyLink provides an assessment, certification, report, or similar material to Customer hereunder, such material is developed in good faith as to its accuracy at the time of inspection or review by CenturyLink and provided AS IS.

7.2 If in CenturyLink's sole discretion (a) Customer is not sufficiently responsive to CenturyLink's requests for information or assistance to allow CenturyLink to properly perform the Service, or (b) CenturyLink determines after commercially reasonable efforts to perform the Service that the Incident is one that the parameters of the Service, including level of effort and number of hours, are not adequate to resolve, CenturyLink will not be required to continue to render the Service.

7.3 The parties acknowledge and agree that any changes to the Client Incident Management Plan during the Service Term become effective on the date of such change, and therefore, Incidents that have occurred prior to such changes will follow the version of the plan that was effective at the start of such Incident.