

CenturyLink Incident Response Service

Networkx Service Overview

Proven incident protection and response

CenturyLink's Incident Response Service (INRS) provides your Agency with a proven, reliable set of people, processes and tools to effectively prepare for and respond to computer security incidents. CenturyLink's INRS offers a custom-engineered solution designed to help your Agency prepare for and quickly address any security event.

Features

CenturyLink's INRS provides an extensive list of features including, but not limited to, the following:

- Web-based, near real-time incident reporting and tracking system
- CenturyLink's Security Operations Center (SOC) is staffed by certified security experts
- CenturyLink's INRS complies with FISMA, FIPS199, IETF-RFC2350, US-CERT and NIST (SP) 800-61 standards
- Detailed threat documentation records show incident information handling from beginning to end, including information that reflects new threats, improved technology and lessons learned during the event
- Robust Security Information Management (SIM) system for correlating and detecting near real-time security threats

Benefits

- CenturyLink's SOC will follow your Agency's standard operating procedures (SOP) when responding to incidents
- CenturyLink's highly skilled and security certified engineers are trained to triage threats and respond quickly and systematically to restore your Agency's network infrastructure after an event
- Consistent, predictable, and effective responses to network threats limit data loss and minimize overall network disruption
- CenturyLink's INRS provides sound documentation and recorded evidence to use for remediation activities that may require legal attention
- Peace of mind knowing that CenturyLink as your trusted partner has a rigorously documented and tested SOP on file and is ready to respond to threats

Geographic availability

CenturyLink's INRS is available world-wide.

How it works

Because CenturyLink has a broad inter-Agency view, this enables our SOC to notify your Agency of threats in advance, thus protecting your Agency from more incidents in the long run. Examples of this support are as follows:

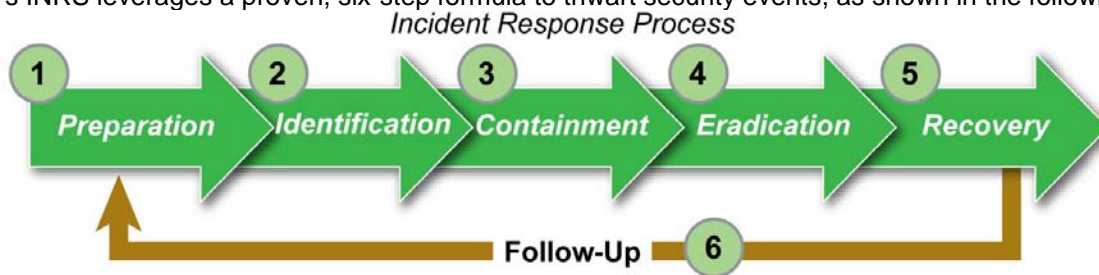
- Fraud/Incident Support - expert, incident-specific support before, during and after investigations of fraud and security incidents; high-level expertise, customized solutions for various incidents, and focus on technical, human and business assessments
- Pre-Incident Planning and Preparation - policy and procedures development and review, organizational assessments, education and awareness training
- During Incident - incident handling and analysis, on-site incident response support and coordination, and, if appropriate, forensics and evidence collection
- Post-Incident - artifact handling, analysis and response, forensic analysis, reports, conclusions and recommendations and aftermath assessment

Contact your CenturyLink Representative today!

Visit GSANetworkx.com and click on "Locate your Account Manager".
Or contact the CenturyLink Customer Support Office: 866-GSA-NETWorx
(866-472-6389) Email: federal@CenturyLink.com



CenturyLink's INRS leverages a proven, six-step formula to thwart security events, as shown in the following table:



009-CQGSMKTG

Steps	Activities Included in CenturyLink's INRS
1. Preparation	<ul style="list-style-type: none"> Assess impacts of viruses and containment efforts Identify software or hardware needed for response Determine types and number of personnel resources needed Develop containment strategy, test it, and reassess its impact Procure items and assign personnel resources identified in assessment phase
2. Identification	<ul style="list-style-type: none"> Identify virus type and assess impact Determine how virus is spread (ports, e-mail, other) using tools such as sniffer traces and logs Develop containment strategy to limit spread Identify critical business users and systems, prioritize clean-up
3. Containment	<ul style="list-style-type: none"> Quarantine all potentially infected PCs by removing them physically from the network Detect and remove virus Apply OS software patch Install/update virus software
4. Eradication	<ul style="list-style-type: none"> Perform a virus scan via a bootable disk, install MS patch, install current virus protection software, and scan Where possible, perform these procedures on critical PCs first Perform quality assessment of each vulnerable PC to ensure that it is clean, protected, and ready to be put back into production
5. Recovery	<ul style="list-style-type: none"> All PCs that have passed the QA procedure are returned to production status and tested Continue monitoring network traffic as warranted
6. Follow-Up	<ul style="list-style-type: none"> Conduct follow-up analysis roundtable discussion Document lessons learned, change preparation plans accordingly

Why buy from CenturyLink?

- CenturyLink provides a comprehensive Incident Response Service that is vendor and device independent. This allows your Agency to retain its current infrastructure and permits simpler future technology refresh.
- CenturyLink's INRS provides a custom-built solution to protect your Agency's infrastructure from malicious Internet content, threats, and breaches, thus freeing limited Agency resources to pursue its more critical missions.
- CenturyLink offers a broad range of expertise in defense modernization efforts, intelligence, homeland security, logistics and product support, health and life sciences, space and earth sciences and global commercial services.

Contact your CenturyLink Representative today!

Visit GSANetworkx.com and click on "Locate your Account Manager".
 Or contact the CenturyLink Customer Support Office: 866-GSA-NETWorx
 (866-472-6389) Email: federal@CenturyLink.com



2011 CenturyLink, Inc. All Rights Reserved. Availability of CenturyLink services varies. Check availability at:

[HTTP://CenturyLink.centurylink.com/legal/docs/availability](http://CenturyLink.centurylink.com/legal/docs/availability).

Not to be distributed or reproduced by anyone other than CenturyLink entities and CenturyLink Channel Alliance members.

Other products available from CenturyLink

CenturyLink provides a comprehensive data protection services portfolio. When combined in a managed service, your Agency benefits with extensive threat mitigation and protection capabilities across its private and public networks. Other Security Services offered by CenturyLink include:

- Managed Firewall Service
- Intrusion Detection and Prevention Services
- Anti-Virus Management Services
- Managed E-Authentication Service
- Secure Managed E-mail Service
- Vulnerability Scanning Service
- Managed Tiered Security Services

Contract Vehicle

Networx Universal & Enterprise

- An overview of CenturyLink's contract is available on the CenturyLink Networx Website at <http://www.gsannetworx.com>

Contact your CenturyLink Representative today!

Visit GSANetworx.com and click on "Locate your Account Manager".
Or contact the CenturyLink Customer Support Office: 866-GSA-NETWorx
(866-472-6389) Email: federal@CenturyLink.com



2011 CenturyLink, Inc. All Rights Reserved. Availability of CenturyLink services varies. Check availability at:

[HTTP://CenturyLink.centurylink.com/legal/docs/availability](http://CenturyLink.centurylink.com/legal/docs/availability).

Not to be distributed or reproduced by anyone other than CenturyLink entities and CenturyLink Channel Alliance members.