iCap Security Response Plan

1. Purpose

The purpose of this policy is to establish a security response plan for EEG business related to the iCap system. This ensures that the security incident management team has all the necessary information to formulate a successful response should a specific security incident occur.

2. Scope

This policy applies to iCap-related configuration, and software deployed either on broadcast closed caption encoders or other embedded equipment, as well as desktop software provided to caption service providers.

Policy

3.1 Service or Product Description

iCap is a network relay service that provides a way for caption service providers to access EEG encoders in a broadcast facility. Individual broadcast entities must specifically authorize each caption service provider they work with to provide access through the iCap system. EEG Support will provide assistance to authorize or de-authorize caption service providers as necessary, however ultimate responsibility for maintenance of correct access lists through the iCap Admin software tool rests with the broadcast entity with an admin account for each encoder.

3.2 Contact Information

In the event of any reported incident relating to the security of the system, customers, employees, or contractors should contact EEG Support immediately at 516-293-7472 and listen to menu options, which may differ between normal business hours and outside normal business hours. Non-critical incidents may be referred to EEG's ticketing system at eegent.com, or emailed to support@eegent.com and/or icapnetworkgroup@eegent.com. Expected response time is judged according to the severity of the incident and/or the customer's Support Tier level, as defined in the customer Support Agreement. Issues affecting the overall security of more than one customer will be promoted to the highest possible priority, regardless of the Support Tier of the individual reporter.

3.3 Triage

EEG Network Engineering and IT Staff will assess the severity of incidents and send a notification to customers as necessary within 24 hours. The availability of an update or a fix may vary by issue and will be of highest priority, with specific details to follow in the customer notifications.

3.4 Identified Mitigations and Testing

All updates to iCap systems including embedded software, desktop software, and iCap Admin, will be subject to special review by the interval Development Security team prior to release, and have a staging period not less than one week in active cluster testing.

4.5 Mitigation and Remediation Timelines

Notification of customers will occur as soon as an issue has been confirmed, unless such notification is deemed to affect the security vulnerability of the system, in which case up to 72 hours for an initial triage may be allotted. All security issues and updates will be treated with the highest priority, with a goal of applying all relevant critical patches within 24 hours.