

Security Incident Policies and Procedures

(AAP recommended policy modified by PCC)

Policy:

It is our policy to record and address attempts to incidentally or intentionally access our physical space and/or the computer system and its components unless such access is authorized by the System Administrator or Security Official.

Procedures:

The practice will designate an individual who will be responsible for implementing and adhering to the practices security incident policies and procedures.

The practice will determine through a variety of security mechanisms, such as User IDs, password protection, anti-virus software, and audit trails when security incidents have occurred.

The practice must periodically monitor user activity, including password activity, virus scans, and audit trails to determine if any security incidents have occurred.

Following the identification of a security incident, the practices first priority must be to communicate the details of the incident to the relevant technical staff or business associates, such as PCC. to expeditiously log and begin resolving the issue.

Once alerted to the incident, the appropriate staff will access the appropriate part of the computer system as quickly as possible. If more than one incident occurs simultaneously, the most critical issue will be addressed first.

The incident(s) will be immediately logged on a security incident log. The practice will take necessary and reasonable steps to respond to and address all identified and confirmed security incidents. All responses will be logged into a security incident log. The log will be kept for six (6) years.

If the incident cannot be resolved and could potentially cause disruptions among other practice employees such that it will inhibit them from performing their assigned job responsibilities, the System Administrator or Security Official will notify the rest of the staff of the situation via email, telephone, verbally, or in writing. The practice should select the communication media that works best under the circumstances. Affected staff will be notified of the estimated time necessary to address the security incident.

Once the issue has been resolved, the System Administrator or Security Official will notify practice staff of the resolution via email, telephone, verbally, or in writing. If there are new procedures which must take place as a result of the reported incident, these must be distributed to practice employees as well. The practice should select the communication media that works best under the circumstances.