R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity~~,~~ at a minimum until the action is complete~~,~~ in support of Requirement R1, Part 1.3. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

Note: The Responsible Entity is not required to retain ~~detailed~~ internal network security monitoring data ~~(full packet capture data, etc.)~~ that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

M2. Examples of evidence may include, but are not limited to, documentation of the internal network security monitoring data retention process(es), system configuration(s), or system-generated report(s) showing data retention with timelines sufficient to support Requirement R1, Part 1.3.

R3. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement ~~R3~~ R2 to mitigate the risks of unauthorized deletion or modification. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

M3. Evidence may include, but is not limited to, documentation demonstrating how internal network security monitoring data is being protected from the risk of unauthorized deletion or modification.