This is what you need to have logging evidence stand up in court.

• Have a clear corporate policy for managing logs across the entire organization.

• Document what is being logged and why, as well as how the log data is captured, stored and analyzed.

• Ensure that 100% of log-able devices and applications are captured and the data is unfiltered.

• Have centralized storage and retention of all logs, with everything in one place and in one format.

• Ensure the time synchronization of logs to facilitate correlating the data and retrieving data over specific timeframes.

• Ensure the separation of duties over logs and log management systems to protect from potential internal threats such as a superuser or administrator turning off or modifying logs to conceal the illicit activity.

• Always maintain backup copies of logs.

• Have a defined retention policy that specifies the retention period across the organization for all log data. Organizations should work with legal counsel to determine the best time frames and have log data incorporated into an overall data retention policy.

• Have a defined procedure to follow after an incident.

• Test the incident response plan, including the retrieval of backup log data from offsite storage.

If an incident or data breach is suspected, there are several steps to take right away:

• Increase the logging capability to the maximum and consider adding a network sniffer to capture additional detail from network traffic. In an incident, it’s better to have more data rather than less.

• Freeze the rotation or destruction of existing logs to prevent the loss of potential evidence.

• Get back up copies of the logs and make sure they are secure.

• Deploy a qualified investigations team to determine the situation.

Source

Musthaler, Linda, and Brian Musthaler. “Using Computer Log Data to Support a Forensic Investigation.” Network World, Network World, 15 May 2009, [www.networkworld.com/article/2254368/using-computer-log-data-to-support-a-forensic-investigation.html.](https://mstate.learn.minnstate.edu/content/2020/4836916-20205000245/www.networkworld.com/article/2254368/using-computer-log-data-to-support-a-forensic-investigation.html.)

Another source says that logging must already be in place and that it is routine logging.  In other words, a network administrator has to already have been logging the network before somebody tries to do something illicit.  There also needs to be several people that can testify that the logging has been going on for a while.  It also says that the logging needs to have backup documents.  For example, a memo or logging plan that has been put into effect.

Source: Hathaway, Annie. “Using Log Data as Forensic Evidence.” Rapid7 Blog, Rapid7 Blog, 19 Aug. 2017, [blog.rapid7.com/2016/08/12/using-log-data-as-forensic-evidence/](https://blog.rapid7.com/2016/08/12/using-log-data-as-forensic-evidence/)