

DOOR ACCESS LOG REQUESTS: APPROPRIATE USES

1. Security Incident

Investigation: A door access log may be needed to investigate a security incident, such as a report of unauthorized access, theft, or property damage in a restricted area.

4. Facilities or Maintenance Review:

Facilities management may request logs to confirm when maintenance staff or other personnel accessed a particular area for repairs or routine checks, ensuring that scheduled work was completed.

2. Monitoring Vendor or Contractor Access:

To ensure compliance with vendor or contractor agreements, access logs may be reviewed to confirm that external parties only accessed the building or specific areas during approved times.

5. Compliance with University Policies:

Door access logs can be used to demonstrate adherence to university security policies, such as restricted access to sensitive areas like laboratories or data centers.

3. Incident of Misuse or Unauthorized

Access: A log may be requested if there is suspicion that someone is accessing areas they are not authorized to enter, or to determine if a specific door was accessed outside of regular hours.

6. Lost or Stolen Badge Investigation:

If a staff member reports a lost or stolen access badge, a log might be requested to check if the card was used improperly or to identify patterns of unauthorized use.

DOOR ACCESS LOG REQUESTS: INAPPROPRIATE USES

1. No Clear Purpose or Justification:

Requesting access logs without a specific or valid reason, such as for curiosity or unnecessary monitoring, is an inappropriate use of resources and could be seen as a violation of privacy.

4. Non-Security-Related Inquiries:

Logs should not be requested for reasons unrelated to security, compliance, or investigations, such as informal tracking of who is using communal spaces like break rooms or conference rooms.

2. Lack of Approval:

If the request has not been approved by the appropriate authority, such as the Department Chair or Director, it should not be submitted. All requests need to be authorized to ensure proper oversight.

5. Personal Conflicts or Disputes:

Access logs should not be requested to resolve personal conflicts or disputes among employees unless there is a formal investigation or HR involvement. Using logs for personal matters is an inappropriate use of the system.

3. Routine Daily Monitoring:

Access logs should not be used for routine tracking of daily employee comings and goings, especially if this monitoring is outside of established HR or security policies. Access logs are not intended for routine employee management.

6. Already Available Information:

If the information can be obtained through other means (e.g., employee time records or schedules), there's no need to request access logs. Duplication of effort should be avoided when other data sources are more relevant.

7. Lack of Relevant Timeframe:

If the request is for a time frame outside of what is relevant to the issue being investigated (e.g., asking for logs far outside the incident window), it may lead to unnecessary data collection.