Automated Compliance Monitoring Log File Formats

Sample CSV Format

Timestamp	User ID	Action	Status	Details
2024-06-13T08:15:21Z	user_0123	LOGIN_ATTEMPT	SUCCESS	IP:192.0.2.5
2024-06-13T08:32:08Z	user_2190	FILE_UPLOAD	FAILURE	Policy violation: File type

```
Timestamp,User ID,Action,Status,Details
2024-06-13T08:15:21Z,user_0123,LOGIN_ATTEMPT,SUCCESS,IP:192.0.2.5
2024-06-13T08:32:08Z,user_2190,FILE_UPLOAD,FAILURE,Policy violation: File type
```

Sample JSON Format

```
[
  {
    "timestamp": "2024-06-13T08:15:21Z",
    "user_id": "user_0123",
    "action": "LOGIN_ATTEMPT",
    "status": "SUCCESS",
    "details": "IP:192.0.2.5"
  },
  {
    "timestamp": "2024-06-13T08:32:08Z",
    "user_id": "user_2190",
    "action": "FILE_UPLOAD",
    "status": "FAILURE",
    "details": "Policy violation: File type"
  }
]
```

Sample Log (Syslog Style) Format

```
2024-06-13T08:15:21Z user_0123 LOGIN_ATTEMPT SUCCESS IP:192.0.2.5
2024-06-13T08:32:08Z user_2190 FILE_UPLOAD FAILURE Policy violation: File type
```

Important Notes

- Ensure timestamp fields use UTC and ISO 8601 format for consistency.
- Log file formats should be documented for auditing and integration purposes.
- Data fields should avoid sensitive information whenever possible, following applicable data privacy regulations.
- Automated log integrity (immutability) is essential for compliance verification.