Key Findings and Evidence
Compliance Investigation Report

Key Findings

1. **Unauthorized Access Detected**
   Evidence indicated multiple instances of unauthorized access to confidential records between March 2 and April 18, 2024.
2. **Lack of Staff Training on Data Security**
   Majority of interviewed personnel were unaware of current data protection protocols, leading to inadvertent sharing of sensitive information.
3. **Failure to Implement Multi-Factor Authentication (MFA)**
   Review of IT controls confirmed that MFA was not enabled for critical user accounts despite policy requirements.
4. **Incident Response Procedure Delays**
   Delayed reporting and escalation of detected incidents did not align with documented response timeframes.

Evidence

- Access logs from IT department showing login activity from unauthorized external IP addresses.
- Employee interview transcripts (Appendix B) citing insufficient awareness of data handling guidelines.
- IT system audit results dated April 24, 2024, highlighting the absence of MFA on 47% of user accounts.
- Email correspondence evidencing a two-day lag between breach detection and official incident report submission.
- Relevant policy documents and compliance manuals reviewed as part of the investigation.

> ## Important Notes
>
> - Findings and evidence should be clearly linked and based on verifiable sources.
> - Maintain objectivity and factual accuracy throughout the document.
> - Secure all sensitive evidence in accordance with data protection regulations.
> - These documents may be subject to legal review; structure and language should be precise and professional.