Case Study

Mr. Neil Network was temporarily employed as a Systems Administrator in the Ministry of Under Sea Cables with privileged access to the organisation's core network infrastructure and internal databases containing sensitive personal and financial information. As part of his duties, Mr. Network was required under the Information Security and Change Management Policies to log all administrative actions taken when managing systems or accessing private databases.

An internal review revealed that on September 12, 2025, Mr. Network accessed the production customer database to perform maintenance using elevated credentials without generating or retaining the required system access logs. Further review showed that on October 3, 2025, Mr. Network queried and exported system performance data from the private financial database without recording the activity in the central audit logging system, contrary to established procedures. Additionally, on October 17, 2025, Mr. Network modified user access permissions within the database management console outside the approved change window and without documenting the actions taken.

Although no evidence of unauthorised data disclosure or misuse was identified, Mr. Network's repeated failure to log administrative actions undermined auditability, accountability, and data protection controls, and constituted a breach of the organisation's IT governance and information security requirements.

Question

Identify the elements of misconduct that would be at the centre of disciplinary charges against Mr. Network?

AND

Generate disciplinary charges against Mr. Network for the infractions described above