Security Policies & CIA Triad

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Policy** | Definition | C | I | A |
| Acceptable Use Policy | Restricts acceptable use of services or resources (e.g., network, systems). Sets behavioural guidelines. |  | X | X |
| Mandatory Vacations | Requires employees to take time off, allowing irregularities or fraud to be detected in their absence. |  | X |  |
| Separation of Duties | Ensures critical tasks are divided among multiple people to prevent fraud and errors. |  | X |  |
| Job Rotation | Employees rotate through roles to detect irregularities and ensure redundancy. |  | X | X |
| Clean Desk Policy | Requires sensitive information to be cleared from workspaces when unattended. | X | X |  |
| Policies related to the Least Privilege Principle | Restrict access rights for users to the bare minimum required for work. Often enforced through IAM in cloud environments. | X | X |  |
| Account Disablement Policy | Specifies timely deactivation of user accounts after they leave or change roles. | X | X |  |
| Never Use Shared Accounts | Prevents multiple users from using the same credentials to maintain accountability. | X | X |  |
| Require Admin to Use Two Accounts | One account for daily use, another for admin tasks. Reduces attack surface. |  | X | X |
| Storage and Retention Policy | Defines how long data is stored and when it should be deleted securely. | X |  |  |
| Social Media Policy | Regulates employee use of social media to protect organization’s reputation and information. |  | X |  |
| Privacy Policy | Explains how personal data is collected, used, stored, and protected. | X | X |  |
| Configuration Management | Maintains system integrity through consistent setup and change control. |  | X | X |
| Disaster Recovery | Outlines how IT services will be restored after a disruption. | X |  | X |
| Incident Response Policies | Describes how incidents are detected, managed, communicated, and reviewed. | X | X | X |