Vendor Contracts

Many vendor contracts include cybersecurity requirements that must be met.
While each vendor contract should be reviewed for specific requirements most contain the following best practices:

A. Password Controls
    I. Two-factor authentication
    II. Safekeeping & frequent password changes
    III. Avoid easy passwords like address, birthday, dog name. Use a partial sentence

B. Access Controls
    I. Mandatory Access Control (MAC)- users have little freedom to determine who has access to their files.
    II. Discretionary Access Control (DAC)- the data owner determines who can access specific resources.
    III. Role-Based Access Control (RBAC)- allows access based on the job title.
    IV. Rule-Based Access Control- best to explain this as an example, only allowing workers to use the computers during a certain time of the day.

C. Network Controls
    I. Monitoring
    II. Network perimeter (e.g., firewalls, intrusion detection and prevention, etc.)
    III. Network access controls

D. Wireless Controls
    I. Must be Wi-Fi Protected Access II (WPA2 or above) compliant.

E. Physical Controls
    I. Vendors should implement secure and controlled physical environment
    II. Environmental and access controls
    III. Physical controls are expected across multiple regulatory requirements and cybersecurity best practice.