Q1

1. Bell-LaPadula model.
    a. Read: Yes
       Write: No
    b. Read: No
       Write: No
    c. Read: No
       Write: No
    d. Read: Yes
       Write: No
    e. Read: Yes
       Write: Yes
2. Dynamic Biba Integrity model.
    a. Remains at Manager, because she is reading from her level.
    b. Remains at Manager, because she is writing to a lower integrity level which doesn't change her level.
    c. Reduced to Intern, because she is reading from a lower integrity level
    d. Unable to perform Write, because she has reduced to Intern level.
    e. Unable to perform Write, because she has reduced to Intern level.

Q2

1. Configure firewall.
    a. Can browse internet
        - *ALLOW 0.0.0.0/0 => 16.35.125.0/24 FROM PORT all TO [80,443] BY TCP*
    b. Kim can SSH into her work device
        - *ALLOW kim_remote_ip=> 16.35.125.25 FROM PORT all TO 22 BY TCP*
            - kim_remote_ip == Remote IP Kim will SSH into
    c. Block incoming traffic from malicious IP address
        - *DENY 85.63.28.0/24 => 16.35.125.0/24 FROM PORT all TO all BY BOTH*
    d. HTTP webserver needs to be globally accessible
        - *ALLOW 0.0.0.0/0 => 16.35.125.13 FROM PORT all TO [80,443] BY TCP*
    e. Allow special DNS server to handle DNS lookups
        - *ALLOW 0.0.0.0/0 => 22.95.33.101 FROM PORT [5000-5100] TO 53 BY UDP*
2. Here, IP spoofing is happening, since the IP addresses are originating from outside the company's internal network. IP spoofing disguises IP packets to appear as if they are coming from a legitimate source within the company's internal network, but, is actually sent from an untrusted external source. To stop IP spoofing, we must implement packet filtering. Drop incoming packets with untrusted source Ips based on their geographical location. Drop outgoing packets that don't originate from the internal network. Also, add Firewall rules to drop external traffic which claims to come from an internal IP address: DENY any to 16.35.125.20.
3. Alternatively, we can use a DMZ, which is an independent network of the internal network firewall, but is also protected by its own firewall. This is an additional layer of security, since it isolates the web server from the internal network. So, even though the web server is compromised, the attacker is still blocked by the internal network's firewall.

To set up the traffic control between the internet, DMZ and the internal network, the firewall should allow incoming internet traffic in order to access just the web server at required ports, which is typically Port 80 and Port 443. Then, we must deny incoming traffic to DMZ from the internal network. Also, outgoing traffic from the DMZ must be controlled to prevent data leaks.

Q4

1. Brute-force attack, since passwords can be 8 chars or longer, users can possibly choose predictable passwords.
2. No, changing the password every 90 days will not prevent attacks. Taking into the fact that MD5 hashes can be computed very quickly, it allows attackers to estimate the password quickly. Can use lookup tables to reverse-MD5-hash the password to get the plaintext password. Given the hashes, if we reverse-hash them using an online tool:
    - 25d55ad283aa400af464c76d713c07ad → 12345678
    - 25f9e794323b453885f5181f1b624d0b → 123456789
    - e807f1fcf82d132f9bb018ca6738a19f → 1234567890

   By doing so, we get another observation that the changed password don't differ much from the previous password, and is a predictable password. If the attacker decides to construct a big lookup table of possible passwords and hash them using an MD5 algorithm, it takes just the same amount of time to guess the password even if you change it or not.
3. To mitigate the vulnerabilities, we can concatenate a unique random salt string to each user's password before hashing it. So, even if two users have the same password, their hashes will differ because of the salts. We can use salt to defend against attacks where the attacker constructs a large lookup table. Since it is very challenging to reverse-engineer the original password without the salt, it makes the size of the lookup table very large, ultimately making them unable to crack users' passwords. Another strategy is to use a stronger hashing algorithm. MD5 is vulnerable to collision attacks, where two different inputs result the same hash, thus making two different passwords indistinguishable. Thus, replacing MD5 with a stronger hashing algorithm, such as SHA-256 and SHA-512, will provide better resistance against collision attacks because they have larger hash sizes.
4. First, the (1) Additional PIN strategy's advantage is that it doesn't require users to carry another device to verify the login. However, it can be guessed or brute-forced if they aren't managed properly. PINs are usually a small set of numbers, thus has a small number of possible combinations, making them easy to attack. Next, the (2) Security Key from Authenticator App strategy's advantage is that provides a higher level of security, because the one-time passwords change every 30-60 seconds, and after it expires, it is no longer valid. However, it has a downside that the user must carry around a separate device to verify the login request via the Authenticator app.
5. MD5 isn't the best algorithm for creating password fingerprints because it is vulnerable to collision attacks. As stated in the response for question 3, this weakness can be exploited by attackers to make the system believe that we are allowing an authorized input, but is unauthorized, by finding a collision that

matches the legitimate hash. Instead, we can use the SHA-256 or SHA-512 hashing algorithm to provide better resistance against collision attacks. They generate longer hash sizes (number of bits in their hash values), thus provides a larger space, making collisions unlikely. Overall, it will offer a much higher level of security compared to MD5.