Question 1.

1a) neither

1b) write access

1c) neither

1d) both

1e) read access

2a) Carols' integrity level stays the same, the integrity levels of the objects she reads to also remain the same.

2b) Carols' integrity level remains the same, the integrity level of the objects **finance** and **equipment** also remain the same, since Carol has a higher integrity level, by glb() they stay at a lower integrity level.

2c) Carols' integrity level changes to that of a **Student** by glb(), the objects **finance and equipment** remain the same

2d) Carol's integrity level remains the same, as Student is lower than Teacher. The object **equipment** now has integrity level **Student**

2e) Carol's integrity level remains the same, as she is reading a file of the same integrity level, the objects remain unmodified and therefore are the same integrity level

Q2)

1. [Rule A] ALLOW 14.20.11.0/25 => 0.0.0.0/0 FROM all TO 80, 443 BY TCP
2. [Rule B] ALLOW 0.0.0.0/0 => 14.20.11.31 FROM all 443 BY TCP
3. [Rule C] ALLOW 0.0.0.0/0 => 14.20.11.0/25 FROM all TO 22 BY TCP
4. [Rule D] ALLOW 14.20.11.0/25 => 54.18.21.22 FROM 6556 to 1552 BY UDP
5. [Rule D] ALLOW 54.18.21.22 => 16.23.18.0/25 FROM 1552 to 6556 BY UDP
6. [Rule E] ALLOW 8.17.21.21 => 14.20.11.81 FROM all to 3221 BY TCP
7. [Rule F] ALLOW 0.0.0.0/0 => 14.20.11.121 FROM > 1023 to 25 BY TCP
8. [Rule F] ALLOW 14.20.11.121 => 0.0.0.0/0 FROM > 1023 to 25 BY TCP
9. [Rule G] ALLOW 14.20.11.0/25 => 14.20.11.0/25 FROM all to all BY BOTH
10. [Rule H] DROP * => FROM all to all BY BOTH

2. IP spoofing. Use filtering rule to prevent spoofed packet from the internet to enter into an internal network. This is not the same as dropping all packets that are coming into the network.

3. DMZ separates the internal LAN from the external network, so in this case the SMTP, IRC and Webpage servers should all be located inside the DMZ. The rest should exist within the internal network zone.

Q3)

1. She can use her password hash file along with the salt to generate a fingerprint. When a fingerprint that exists in the system is generated she now knows the username and password of this user, and can now log into the system. More specifically, 1. Choose a password, 2. Hash this password, apply Salt (from fingerprint file), 3. Find matching fingerprint, 4. Obtain username, 5. Login

It would take (assuming the worst case scenario,), 100, 000 multiplied by 250, 000 password entries = 25,000,000,000 attempts, that is taking 1 password, applying he has, and then applying the Salt for each fingerprint to see if there is a match.

2. use a more complex hash function that is expensive to compute, such as with bcrypt, or one that uses a lot of memory, such as crypt. Use a salt that is greater than 8-bits.