Make sure when you take evidence date and IP/host must be visible

# **Device detail**

**IP address and Domain screenshot >**

**Please paste the screenshot**

# **Services (services.msc>running services) > Q21**

**Make sure you cover the IP address or hostname in screenshot.**

**Please paste the screenshot**

# **Listening Ports (netstat -an | findstr LISTENING) > Q21**

**Please paste the screenshot**

# **Local account and administrator including full user list>** **> Q45**

# Make sure default account must be disabled e.g. administrator and guest]

**Please paste the screenshot**

# **Antivirus > Q31 & 32**

* Version

**Please paste the screenshot**

* Update schedule and Signature version

**Please paste the screenshot**

* Scan schedule

**Please paste the screenshot**

* Log setting:

**Please paste the screenshot**

av running and cannot disable by user:

**Please paste the screenshot**

# **Patch [Make sure patch must be updated] > Q34**

**Please paste the screenshot**

# **Below is the PCI parameter for Password and account lockout.**

PCI DSS v 3.2.1

Account lockout duration - 30 min  
Account lockout threshold - 6   
Session timeout policy - 15 min  
Password length - 7  
Password complexity -enabled (numeric and alphabetic characters.)  
Password history - Last 4  
Password expiry - 90 days

PCI DSS v 4.0

Account lockout duration - 30 minutes or until the account is reset by an administrator

Account lockout threshold - 10 unsuccessful login attempts

Inactive session timeout - 15 min

Minimum password length - 12 (8 characters if the system does not support 12)

Password complexity - enabled (numeric digits and alphabetic characters)

Password history - Last 4

Password expiry - 90 days

If a password is generated for new user or the password is reset, the generated password must be unique for every user and it must be changed after the first use.

# **Password Policy and Account lockout policy > Q50**

**Show the integration with Domain or if it is configured local paste screenshot.**

# **Session Timeout (gpedit.msc>Windows Settings>Security Settings>Local Policies> Security options> Microsoft Network server: Amount of idle time required before suspending session) > Q50**

**Show the integration with Domain or if it is configured local paste screenshot.**

# **Password encryption during transmission (Q51)**

**RDP over TLS**

<Paste screenshot below>- refer below command and screenshot.

gpedit.msc>Administrative templates>Windows components>Remote desktop services> remote desktop session host>Security

**Show the integration with Domain or if it is configured local paste screenshot.**

# **Audit Policy > Q67**

**Please paste the screenshot – Show the integration with Domain**

# **NTP [(w32tm /query /status)] > Q69**

**Please paste the screenshot**

# **Last login since 90 days > Q48**

**Inactive users (90 days) – Provide procedure and policy also evidence from AD.**

**Note: If there is more than 1 Domain in the entity and if it is not sampled make sure provide the full output of Password policy, account lockout policy, RDP over TLS**

# **Q18- Personal Firewall/ User cannot disable personal FW**

**If personal firewall is controlled by AV, please paste settings screenshots**