If the U.S. government is funding or providing commercial Wi-Fi for military dorm residents, there are often cybersecurity, privacy, and contractual requirements—but the exact requirements depend on who owns and operates the network.

There are generally three common scenarios:

1. Commercial ISP provides the service (such as Boingo or another contracted provider).
2. The installation or base network office manages the service.
3. A hybrid arrangement where the government pays but a commercial company operates the infrastructure.

The requirements differ significantly in each case.

Generally speaking:

- Logging: Most providers maintain network logs such as IP address assignments, connection times, authentication events, and network performance data. Deep inspection of content is generally not required unless specified by contract or necessary for security or legal reasons.
- Data retention: There is no single government-wide retention period for dorm internet. Retention is usually determined by:
  - the service contract,
  - company policy,
  - applicable federal and state laws,
  - and any DoD-specific requirements if they apply.
- Privacy: If residents use a government-managed network, they should expect limited privacy and are typically presented with a banner or acceptable use policy. If it is a commercial provider, privacy is primarily governed by the provider's privacy policy and contract.
- Abuse handling: Providers generally need procedures for responding to:
  - copyright complaints (DMCA),
  - malware or botnet activity,
  - spam,
  - harassment or illegal activity,
  - law enforcement requests.
- Cybersecurity incident reporting: If the provider is operating under a DoD contract, the contract may require reporting certain cyber incidents involving covered defense information or contractor systems. Requirements vary based on the contract and applicable regulations, such as those in the Defense Federal Acquisition Regulation Supplement (DFARS). If the network is purely commercial with no covered government information, normal commercial incident reporting requirements may apply instead.

If you're asking from the perspective of developing or reviewing a contract for government-funded dorm internet, you would typically consider requirements in areas such as:

- Audit logging
- Log protection and integrity
- Log retention periods
- Incident response procedures
- Security monitoring
- Privacy notices
- Acceptable use policy
- Vulnerability management
- Security patching
- Law enforcement cooperation
- Cyber incident notification timelines
- Data disposal at the end of retention periods