4.

20. networks and while residing at rest on storage media on-site and off-site, on computer systems, and district mobile devices including laptops, tablets, and mobile telephones.
21. Maintain the proper physical security mechanisms for the protection of information processing and storage facilities containing Sensitive Data, that are intended to protect such facilities from unauthorized access, damage, or interference.
22. Maintain accountability measures and security mechanisms at all times to control remote access to the District's systems and networks during external remote access use. External connections to the District's network must be established securely in order to preserve the integrity and availability of the network, including the integrity of data transmitted over the network.
23. Maintain incident response procedures, and respond to cyber-security incidents in a timely, thorough, and compliant manner.
24. Ensure that the District's cybersecurity capabilities are current and effective through periodic testing, audits, and internal and external reviews.