NCA-01.040824: NCERT Advisory – CCTV Camera Safe Usage Guidelines

Introduction. CCTV camera usage has become indispensable in offices and residential areas. However, where it offers ease of use/remote view from anywhere around the world (via internet), CCTV cameras are at the same time a cyber and physical security risk. A few recommendations on safe usage of CCTV network are appended below for adherence.

Recommendations. Following are cyber security best practices/safety guidelines for CCTV administrators and end users:

a. **CCTV Administrators**

(1) **Avoid Unnecessary Remote View**. Do not provide CCTV remote view access unnecessarily. In case, remote access is necessary, ensure strong passwords, device MAC filtering etc. on devices being used for remote access and remote access portal.

(2) **Access Control**. Limit access of CCTV camera system to only authorized administrators. Implement strong authentication mechanisms and follow the principle of least privilege.

(3) **Regular Auditing**. Conduct regular audits of user access logs, camera configurations and system settings. This helps in identification and addressing potential security vulnerabilities/ suspicious activities.

(4) **Network Segmentation**. Isolate the CCTV camera network from other critical networks to minimize risk of lateral movement by potential attackers.

(5) **Firm wares and Software Updates**. Keep camera firm ware and software up to date to patch known vulnerabilities. Regularly check for updates from manufacturers and apply them promptly.

(6) **Incident Response Plan**. Develop and regularly update an incident response plan specific to the CCTV camera system. This ensures a swift and effective response to security incidents.

(7) **Encryption**. Enable encryption for both data in transit and data at rest. This adds an additional layer of protection against unauthorized access.

(8) **Monitoring and Alerts**. Implement continuous monitoring for the CCTV system and set up alerts for any suspicious activities. Early detection can help to prevent or mitigate potential security threats.

(9) **Vendor Guidelines**. Adhere to security guidelines provided by camera manufacturers. Stay informed about any security advisories or patches released by vendors.

b. **CCTV End Users**

(1) **User Training**. Educate end-users about the proper use of CCTV cameras and the potential security risks associated with them. Encourage the use of strong passwords and secure authentication practices e.g. OTP remote view.

(2) **Privacy Awareness**. Make end-users aware of privacy considerations related to CCTV cameras. Avoid placing cameras in sensitive areas and ensure that they are used responsibly.

(3) **Secure Passwords**. If end-users have access to camera settings, ensure that they use strong, unique passwords. Discourage the sharing of passwords and emphasize the importance of password hygiene.

(4) **Reporting Suspicious Activity**. Encourage end-users to report any suspicious or unusual activities related to the CCTV system promptly. This helps in the early detection of potential security incidents.

(5) **Physical Security**. If end-users have physical access to cameras, stress the importance of maintaining the physical security of the devices. Tampering with cameras could compromise the entire surveillance system.

(6) **Privacy Filters**. Consider implementing privacy filters or controls to limit the exposure of certain areas, addressing concerns about unintentional or intrusive monitoring.

(7) **Compliance with Policies**. Ensure that end-users are aware of and comply with organizational policies related to CCTV camera usage and cybersecurity practices.