Risks, Threats, Attacks, and Related Incidents & Events

For [company name] to be able to adequately respond to cybersecurity occurrences, all users (i.e., employees, contractors, vendors, guests, etc.) need to be aware of the following risks, threats, attacks, and related incidents that can cause significant damage to organizational assets:

- **Cyber Intrusion:** The unauthorized act of spying, surveilling, and the possible theft of information and/or damage to information systems.

- **Ransomware:** A type of malicious software that essentially blocks access to the victim's data or threatens to publish or delete it until a ransom is paid.

- **Malware:** An umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.

- **Watering Hole:** A computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group gets infected. The malware used in these attacks typically collects information on the user.

- **Phishing:** The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords, credit card numbers, Personally Identifiable Information (PII), and other data deemed sensitive and confidential.

- **Spoofing Attack:** An event in which one person or program successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage.

- **Web Application Development Security Risks:** These are risk associated with developing software used for web facing systems, such as e-commerce servers, publicly accessible servers that provide general content, and other forms of information that are "public" facing within the untrusted Internet. Learn more at https://www.owasp.org about such threats.

- **Denial of Service (DoS) Attack:** A cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

- **Distributed Denial of Service (DDoS):** A type of a type of Denial of Service Attack (DoS) where multiple compromised systems are used to target a single system causing a Denial of Service (DoS) attack.

- **Credential Reuse:** A cyber incident whereby account credentials are leaked from one website, and because users often use the exact same or similar passwords on multiple websites, those accounts are then also compromised.
- **Deliberate, Unauthorized Access Attempts:** Abuse by an individual to gain access to a system by continuing to enter a username and password until they are effectively locked out or ultimately denied.

- **Session Hijacking and Man-in-the-Middle (MITM) Attacks:** The exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer. Simply stated, any attack that involves the exploitation of a session between devices is session hijacking, with the "session" being a connection between devices in which there is state.

- **Hacktivism:** The subversive use of computers and computer networks to promote a political agenda.

- **Drone Jacking:** The hijacking of a drone, either by physically capturing the device or by compromising its navigation system.

- **Social Engineering:** The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purpose.

- **Insider Threats:** A malicious threat to an organization that comes from people within the actual organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems.

- **Acceptable Use Violations:** Violating an organization's usage rights to information systems.

- **Loss or Theft of Assets:** Assets (such as physical assets, along with data and information) that is either physically or electronically lost or stolen.

- **Loss of Sensitive Data:** The loss (i.e., theft or unauthorized use) of data, which includes, but is not limited to the following: Protected Health Information (PHI), Personally Identifiable Information

(PII), Personally Identifiable Financial Information (PIFI), cardholder data, and other types of data deemed personal/confidential, etc.

- **Rogue Software:** A form of malicious software and Internet fraud that misleads users into believing there is a virus on their computer, and manipulates them into paying money for a fake malware removal tool (that actually introduces malware to the computer). It is a form of scareware that manipulates users through fear, and a form of ransomware.

- **Drive-by-Downloads:** The unintentional download of a virus or malicious software (malware) onto a system. A drive-by attack will usually take advantage of (or "exploit") a browser, app, or operating system that is out of date and has a security flaw.

- **Malvertizing:** The use of online advertising to spread malware by injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages.

- **Advanced Persistent Threats:** A network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization.

- **Other:** Any other risk, threat, attack, and related incident not discussed in the above listed descriptions.