Incident Clarification	Incident Category	Description	Technical Support	Advisory Support	Response Time	Priority
1. Availability	1.1 DOS	A denial of service (DOS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In a distributed denial-of-service, large numbers of compromised systems (sometimes called a botnet) attack a single target.	Yes	Yes	6 Hours	1 - Very High
	1.2 DDOS					
2. Intrusions	2.1 Account Compromise*	An account compromise is the unauthorized use of a computer account by someone other than the account owner, might expose the victim to serious data loss, data theft, or theft of services.	Yes	Yes	12 Hours	2 - High
	2.2 Defacement	Defacement is an attack on a website or on a computer application that changes the visual appearance. These are typically the work of defacers, who break into a web server and replace the hosted website with one of their own.	Yes	Yes	12 Hours	2 - High
	2.3 Exploiting Known Vulnerability	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardized identifier such as CVE name (e.g. buffer overflow, backdoor, cross site scripting, etc.).	Yes	Yes	12 Hours	2 - High
	2.4 Login Attempts	Multiple login attempts (Guessing / Cracking of passwords, Brute force).	Yes	Yes	24 Hours	3 – Medium
3. Information Content Security	3.1 Unauthorized Access and Modifications to Information*	Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore, attacks are possible that intercept and access information during transmission (wiretapping, spoofing or hijacking). Human/configuration/software error can also be the cause.	Yes	Yes	12 Hours	2 - High
4. Information Gathering	4.1 Scanning	Attacks that send requests to a system to discover weak points, gather information about hosts, services and accounts.	Yes	Yes	48 Hours	4 - Low
	4.2 Sniffing	Observing and recording of network traffic. (wiretapping)	Yes	Yes	24 Hours	3 – Medium
	4.3 Social Engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats)	No	Yes	48 Hours	4 - Low

5. Fraud	5.1 Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (E.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes).	Yes	Yes	24 Hours	3 – Medium
	5.2 Copyright	Offering or Installing copies of unlicensed commercial software or other copyright protected materials.	No	Yes	48 Hours	4 - Low
	5.3 Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.	No	No	48 Hours	4 - Low
	5.4 Phishing	Masquerading as another entity in order to persuade the user to reveal a private credential.	Yes	Yes	12 Hours	2 - High
	5.6 Scam	Scams are one of the most common types of fake emails, text messages, calls, or social networking message with the intention of financial fraud. (Lottery, Inheritance, Job, Green Card, BMW, Coca-Cola, Facebook Gifts, etc.)	No	Yes	48 Hours	4 - Low
6. Malicious Code	6.1 Virus	Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system.	No	Yes	24 Hours	3 - Medium
	6.2 Worm	A computer worm is a type of malicious software program whose primary function is to infect other computers while remaining active on infected systems.				
	6.3 Trojan	A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems.				
	6.4 Spyware	Spyware is unwanted software that infiltrates your computing device, stealing your internet usage data and sensitive information.				
	6.5 Dialler	Another type of dialer is a computer program which creates a connection to the Internet or another computer network over the analog telephone or Integrated Services Digital Network.				
	6.6 Rootkit	A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or an area of its software that is not otherwise allowed and often masks its existence or the existence of other software.				

	6.6 Ransomware	Ransomware is a type of malware from crypto virology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.				
7. Abusive Content (Cyber Harassment)	7.1 Spam	Spam or "Unsolicited Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content.	No	Yes	48 Hours	4 - Low
	7.2 Harmful Speech	Discretization or discrimination of somebody (e.g. cyber stalking, racism and threats against one or more individuals).	No	Yes		
	7.3 Fake Accounts	Include social media, email services, etc.	Yes	Yes		
	7.4 Child/Sexual/Violence	Child pornography, glorification of violence, etc.	No	Yes		
	7.5 Cyber Bulling and Stalking	Cyberbullying or cyber harassment is a form of bullying or harassment using electronic means. Cyberbullying and cyber harassment are also known as online bullying.	No	Yes		
	7.6 Religious	Form of harassment, usually consisting of invective and potentially intimidating or threatening comments towards victims. Often contains exceptionally abusive, foul or otherwise hurtful language.	No	Yes		
	7.7 Racial					
8. Other	All incidents which do not in one of the given categories should be put into this class	To be decided by the Sri Lanka CERT|CC				