Marking Scheme of Private Security for Model Question of Class 11th Level 3: -

Ser No	Answer	Marks
1.	1.Unauthorized access − an unauthorized access is when someone gains access to a server, website, or other sensitive data using someone else's account details. 2. Hacker − Is a Person who tries and exploits a computer system for a reason which can be money, a social cause, fun etc. 3. Threat −Is an action or event that might compromise the security. 4. Vulnerability − It is a weakness, a design problem or implementationerror in a system that can lead to an unexpected and undesirable eventregarding security system. 5. Attack −Is an assault on the system security that is delivered by a personor a machine to a system. It violates security. 6. Antivirus or Antimalware −Is a software that operates on different OSwhich is used to prevent from malicious software. 7. Social Engineering −Is a technique that a hacker uses to stole data by aperson for different for purposes by psychological manipulationcombined with social scenes. 8. Virus − It is a malicious software that installs on your computer withoutyour consent for a bad purpose. 9. Firewall − It is a software or hardware which is used to filter networktraffic based on rules. Or 1. Computer Application White listening −The idea is to install just arestricted number of applications in your computers, which are useful aswell as are genuine. 2. Computer System Restore Solution − In case your computer is hacked,and your files are damaged, you should have the possibility to again haveaccess to your files. An example is Windows System Restore or Backup. 3. Computer and Network Authentication −The data that is accessed overthe network is best to be provided only to the authorized users. Useusernames and passwords!!! 4. File, Disk and Removable Media Encryption − Generally a good practiceis to encrypt hard disks or removable devices, the idea behind this is incase your laptop or your removable USB is stolen, and it is plugged inanother machine it cannot be read. A good tool for this is True crypt. 5. Remote Access Authentication − Systems which are accessed over thenetwork is best to be provided only to the authorized users. Useusernames and passwords!!! 6. Network Folder Encryption − Again like the case of NetworkAuthentication, if you have a network storage or a network foldershared, it is good to be encrypted to prevent any unauthorized user whois listening to the network to read the information. 7. Secure Boundary and End-To-End Messaging − Nowadays email orinstantmessaging is widely spread, and it is the number one tool tocommunicate. It is better that the communication to be encryptedbetween the end users, a good tool for this is PGP Encryption Tool.	5
2.	It should be noted that evidence can be both oral and documentary and,electronic records can be presented in the court as evidence, which means thateven in criminal cases, evidence can be presented by way of electronic records.This shall include videoconferencing. 1. Oral Evidence: -Oral evidence renders to the evidence that is mainly words spoken by mouth. It isadequate to be proved without the support of any documentaryevidence,provided it has credibility. 2. Documentary Evidence: -Docuevidence is the evidence that mentions any issue described orexpressed upon any material by way of letters, figures, or marks or by more thanone of the ways which can be used for recording the issue. Such evidence ispresented in the form of a document to prove a disputed fact in court. Or	5

	Tools Used in Forensic Analysis: Whether you require forensic analysis for an investigation into unauthorizedserver access, a human resource case, or a high-profile data breach investigation,these open-source digital forensic tools can help carry out memory forensicanalysis, forensic image exploration, hard drive analysis, and mobile forensics. Thetools give ability to retrieve in-depth information about an infrastructure.Here are some of them: 1. Autopsy: It is an open-source GUI-based tool that analyzes smart phones andhard drives. It is used worldwide for investigating what happened in a computer. 2. Wire shark: It is a network capture and analyzer software tool that sees whathappens in the network. 3. Encrypted Disk Detector: It helps in checking encrypted physical drives andsupports Bit locker, True Crypt, and Safe boot. 4. Magnet RAM Capture: It is used to capture physical memory of a computer toanalyze memory artifacts. 5. Network Miner: It is a network forensic analyzer for Linux, Windows, and MacOSX for detecting operating systems, hostname, open ports, and sessions by PCAPfile or through packet sniffing.	
3.	Security Equipment's by Security Personal: 1. Flashlight: A flashlight is a piece of must-have security equipment during day or nightboth. Security guards carry different-sized flashlights for their duties. It may sound unnecessary, but security guards need flashlights during brightdaylight as well. The reason is they have to secure buildings and tackleunexpected power outages. They have to escort people in and out of the areaand that needs proper light. Flashlights also work best in noisy places where security guards cannotcommunicate with each other effectively. In this case, the mode ofcommunication is the flashlight with which they get the attention of theirfellows. Small flashlights with long-lasting batteries and the brightest light arethe best to carry. 2. Personal Audio Recorder: Security guards should carry personal audio recorders to record all thehappening during their duty hours. The audio recorder helps security guardsquickly record any suspected activity without having to write down all thedetails. The audio recording is useful to maintain the log and keep an eye on all thehappenings. Personal audio recorders of a security guard also make them lookmore professional and truly help them to effectively respond to anyunexpected scenarios. An audio recorder is a great tool to record all the happenings during mobilepatrolling. The security guards don't have to use writing tools while driving.They just must record their audio on the recorder and make patrolling asefficient as possible. 3. Writing Tools:Although there are numerous effective devices that help record importantscenarios during duty hours. But let's face the fact: these devices might breakor become faulty and don't respond at all when needed. That is why it's essential for security guards to carry the good old pen andpaper. This will help them to record important happenings even if their audiorecorder is not functioning properly. 4. Security Communication Equipment: Communication is the key to survival for security guards in various securitysituations. So, security guards must carry functional communicationequipment, along with security guard training that helps them communicatewith their fellows when needed. The most used and beneficial communication equipment forsecurity guards is a two-way radio. The two-way radio is a simplecommunication tool that must be carried by every security guard so that theycan ask for help and communicate with fellow security guards when needed.	5

	5. Earpiece: Security guards should use an earpiece with their two-way radios to not onlycommunicate effectively but also perform the duties well as their hands wouldbe free. Wireless earpieces are the best option for security guards to maintaincommunication and use their hands at the same time. The earpiece comes indifferent shapes and sizes. The security guards should be given an earpiece depending upon the nature of their duty and security situations that mightarise. 6. Wearable Body Cams: Body cameras help security guards to record every second of their duty hours.This helps to record the faces of criminals, securities situations, and liabilitymakes them look more professional. Although personal body cameras are an important tool for security personal, yetthe guards should be aware of when they cannot use body cameras torecord people. This is the reason we consider this item as a must in the list ofsecurity guard equipment. 7. Comfortable Security Boots: Security guards aren't meant to sit all day. You will find security guards always on their feet. And to perform their duties well they need footwear that is protective and comfortable as well. This helps them to be on their feet and walk without any hurdles. 8. First Aid Kit: Security guards should be prepared for any unexpected security situation. Thatis why a first aid kit is important to carry along. The first aid kit should haveover-the-counter pain medications, band aids, and other important medicinesthat would be helpful when needed. The first aid kit is not only beneficial for the security guard team but also forpeople when any security situation arises. The security guards should not onlycarry the first aid kit, but they should also know when and how to use the kit. Or 1. Being a visible authoritarian figure capable of deterrence. 2. Enforcing laws and regulations related to trespassing. 3. Guarding high-traffic areas and monitoring all visitors. 4. Checking the identification or passes of visitors or issuing them passes. 5. Taking charge of metal detector and bag-checking security procedures. 6. Preventing access to and photo in forbidden areas. 7. Performing routine inspections in the areas they are guarding. 8. Securing specific areas during maintenance work and emergencies. 9. Monitoring activities on security camera video monitors. 10. Staying alert and observant, and reporting suspicious activities 11. Recognizing potential threats and taking steps to mitigate them. 12. Responding to emergencies. 13. Participating in rescue operations with firefighters and police. 14. Detecting criminal or dangerous and detaining possible suspects. 15. Informing the police about the criminal incidents. 16. Summoning the paramedics in case of assaults and injuries. 17. Advising people about necessary safety precautions.	
4.	Martial Arts Skill:It may be necessary for security guards to protect clients andtheir assets from physical attacks by taking direct action against the attackers.	3
5.	Bullet CCTV cameras have a long cylindrical shape, giving them theirname and a distinctive look. This look is recognizable to nearly everyoneand thus acts as a deterrent to unwanted individuals.The bullet CCTV cameras are shielded against dust, dirt, and other naturalelements. The cameras can easily be mounted with a mounting bracket. Main benefits of bullet CCTV cameras: (i) Highly visible means it acts as a deterrent (ii) More resistant against elements (rain, dust) (iii) Compact size aids installation	3
6.	Switch:Ethernet switch network devices are one of the more advanced networking devices that connect multiple devices to a LAN using Ethernet cables. This isone of	3

	the best network connection devices. Unlike Ethernet hubs, switchescan analyze data packets and forward them only to the device that needsthem, which reduces network congestion and improves performance.Switches can also be managed, allowing network administrators to monitorand control traffic. This is also one of the best types of network devices.	
7.	Routers: Routers are great networking devices that connect a range of devices in alocal area network (LAN) and that LAN to the internet. Router network deviceis one of the best connection devices. Routers analyze the data sent betweendevices and forward it to the correct destination. They can also act as afirewall, blocking unauthorized access to the network. Most routers have abuilt-in Wi-Fi access point, which allows wireless devices to connect to thenetwork.	3
8.	Video Surveillance Systems:Video surveillance solutions are one of the most crucial parts of public safetyaccess control. These systems use cameras and other sensors to areas forsuspicious activities and potential threats. The video that's captured can alsohelp authorities quickly respond to emergencies and identify suspects incriminal investigations, while security and public safety personnel can useadvanced video analytics to detect anomalies and potential threats in real time. Or Cyber security Solutions: As more municipalities connect to the internet via the IoT and smart citytechnologies, they become vulnerable to cyber-attacks that could compromisepublic safety. Robust cyber security measures, such as firewalls, intrusiondetection and prevention systems, and security protocols, can help eliminateintrusions and secure confidential information. Public safety access control is a critical aspect of ensuring public safety.Biometric identification systems, video surveillance, access controltechnologies, and cyber security measures are just a few technologies that canbe used to create a comprehensive public safety access control system. Byimplementing these technologies, authorities can monitor and control accessto public spaces, buildings, and infrastructure, respond quickly to emergencies,and prevent potential threats to public safety.	3
9.	What is Public Security:Public security is a service provided by the government that includes police,detectives, federal officials, and other public security officials. The publicsector's main concern is the safety of the public since they are notfunded by a private organization. This also means that public officers mustoperate within certain governmental standards and restrictions but have theauthority to arrest. Or What is Private Security:Private security is a privately owned security service that is hired by specificclients instead of being funded by a government. Private security guards oftenhave strict training and certification standards. Despite this, they are devoid ofpower and authority to detain or arrest anyone.	3
10.	Hacker is a Person who tries and exploits a computer system for areason which can be money, a social cause, fun etc.	2
11.	Virusis a malicious software that installs on your computer withoutyour consent for a bad purpose.	2
12.	Analog Camera**:** An analog system uses a coax cable to send video signals backto the central controller unit or DVR.	2
13.	Image Tampering:Image tampering is a digital art which needs understanding of image propertiesand good visual creativity. One tampers images for various reasons either to enjoyfun of digital works creating incredible photos or to produce false evidence.	2
14.	Digital Camera: Digital systems are more efficient because they digitize the signal before sending it. Or Network IP: A network IP system can use either analog or digital cameras anduses a video server to stream the video over the internet to its destination.	2

15.	CCTV Footage can be edited:No matter what reason, you can edit CCTV videos easily. To edit CCTV footage,CCTV video editing software is needed. If you have not yet found a suitable tool toedit CCTV videos, the following are some best software mentioned to edit videos. Or CCTV Law in India: Section 67 & 67A of the IT Act, 2000: If CCTV footage isobscene or sexually explicit, and it is published or transmitted, these provisionsare applicable. In case of obscenity, Section 67 provides for up to three yearsimprisonment and a fine of up to ₹5 lakhs.	2
16.	(A) 2005	1
17.	(C) 144	1
18.	(C) Ctrl + V	1
19.	(B) Property	1
20.	(C) Expired	1
21.	(D) Writing	1
22.	Permanent Account Number	1
23.	Local Area Network	1
24.	Unarmed Security Guard	1
25.	National Green Tribunal	1
26.	Closed Circuit Television	1
27.	Standard Operating Procedure	1
28.	Operating System	1
29.	True	1
30.	True	1