

SETTING UP A DETEX GUARD TOUR SYSTEM

General

As a general statement, the purpose of a guard tour system is to ensure that security officers are present at specific locations at specific time intervals; to prove that the officers were or were not present at those locations at those time intervals; and to provide documentation of those facts. The guard tour system may, as an option, allow the documentation to (1) indicate the names of the officers performing the tours, and (2) permit the officers to record events or conditions that they observe while performing the tours. Such events or conditions ("incidents") generally pertain to security, safety, maintenance or operational issues.

Guard Tour System Components

A Detex guard tour system consists of data points (magnetic data strips or RFID tags), one of which is physically installed at each location that an officer is to visit. The officer carries a device to read the data point at each location ("checkpoint"); this device is referred to as the "data acquisition unit" (DAU). In the Detex systems, this device may be the "Escorte" (which reads magnetic data strips) or the "ProxiPen" (which reads RFID tags). As the officer visits each checkpoint and reads the data point, the DAU records the time, date and the data point's unique identification number.

The Detex guard tour system also includes a device for downloading the data acquired during the tour from the DAU. This device is referred to as the "data transfer unit" (DTU).

Most Detex guard tour systems also include software that produces reports of the officers' activities, thus requiring that the client provide a computer on which the software may be installed. This can be either a standalone PC or a workstation in a network. The Detex "Patrol Manager" system is an exception in that it permits the DAU to transfer the tour report directly to a printer without the need for a computer.

The guard tour software translates the downloaded data into a report that documents each tour that was performed and indicates the time and date that each checkpoint was visited. The report also highlights any checkpoints that were not visited ("missing"), any that were visited more often than required ("double" or "multiple"), and any from another tour that should not have been visited. As mentioned above, the report may optionally include the names of the officers who performed the tours and any incidents that the officer observed during the tour. The report usually concludes with a numerical summary of the tour activity included in that report.

Establishing the Tour(s)

If the client is upgrading a Detex guard tour system or changing over from a competitor's system, the officer tours are probably already established. However, if the client does not have an existing guard tour system, it must be determined how many tours are needed and which checkpoints are to be included in each tour. The client must also decide how often and when he wishes to download the tour data and prepare the tour activity reports.

These parameters are based solely on the client's needs and wishes. The client obviously has reasons for employing security officers, and already knows what tasks they are to perform and how often they should be done. The establishment of the tours is simply a process of organizing and formalizing those tasks.

A guard tour generally consists of a set of locations (“checkpoints”) that an officer is to visit at specified time intervals. The officer usually visits each checkpoint once during each tour, although the tour may be configured so that multiple visits to specific checkpoints are required.

Some Detex guard tour software programs also permit the designation of checkpoints as “optional;” that is, they are to be visited by the officer if time permits, but are not identified as “missing” if the officer is unable to visit them.

The Detex guard tour systems require that each tour begin with a unique checkpoint that cannot be used as a part of any other tour. This “start point” identifies the tour to the software and simplifies the reporting logic by making it easier to identify “exceptions” (missing, double or multiple checkpoint readings, etc.). It is essential that an officer begin any and every tour by first reading the “start point” for that tour. The start point may be the first checkpoint in the tour, if it is intended that the tour always begin at that point; or it may be mounted in another location (a guard shack, for example) if it is desirable that the tour not always be performed in the same order.

When setting up the guard tour system, the client may create only one tour, if that meets his needs, or he may create multiple tours. One factor in this decision is what the client wants to see in the tour reports. If he has a large facility but anticipates that in some cases he will only want a report of officer activities in a certain area, then a tour should be created including only that area; the same goes for any other similar areas.

The client may also create tours that are similar, including some (but perhaps not all) of the same control points and adding others, as long as each tour is assigned its own unique starting data point and is given a suitably descriptive name in the software. For example, the client might want a tour performed in one way during the week but a slightly different way on weekends, holidays or during plant shutdowns.

Setting Up the System

The first step in setting up the guard tour system is for the client to prepare a list of the tours that the security officers are to perform and the checkpoints that are to be included in each tour. The checkpoints are generally described by their physical location, and this description should be included for each checkpoint. Each tour should also be given a descriptive title.

If the client wishes to use data points for identifying the officers, he should prepare a list of the officers’ names that are to be assigned to the data points. In practice, the officer will typically read his own identifying data point with the DAU before he begins his first tour. The software then lists that officer’s name in the report at the beginning of that tour and every subsequent tour, until either (1) another officer’s identifying data point is read with that same DAU, or (2) the DAU’s data memory is cleared.

Where these officer identification data points are physically located is determined by where the officers transfer the DAU from one to another (at a shift change, for example). If the officers normally begin tours from one physical location (a guard shack or security office, for example), and this location is where the DAU’s are kept and/or transferred between officers, then the officer identification data points might be physically mounted in that location on a board, wall, etc. If the officers are mobile and normally transfer the DAU between officers at remote locations, then the

officer identification data points might be mounted on a plastic card that the officer carries with him, as an example.

If the client wishes to have officers record incidents that they observe while performing the tours, he should prepare a list of the incident descriptions that he wants to appear in the tour reports. Incidents are recorded by having the officer carry a wallet-sized "incident book" with him while performing the tours. The incident book contains a number of data points (20 for the Escorte, 12 for the ProxiPen); each data point is assigned a description in the guard tour software. A list of the descriptions for each data point is written into the incident book. As the officer performs the tour, if he observes an event or condition described in the incident book, he first reads with the DAU the checkpoint that identifies his location, then reads the data point in the incident book that describes the incident.

With these lists of tours and checkpoint descriptions (and, if desired, officer names and incident descriptions) in hand, the next step is to install the guard tour software on the client's computer. The data transfer unit should be connected to the computer (either to a serial port or USB port) and the DTU's power supply connected to the DTU and to power. In the ProxiPen system, it is then necessary to configure the DTU (primarily to set the correct time zone).

The DAU (either Escorte or ProxiPen) should be placed in the DTU and interrogated with the software's utility function. This function is used to configure the DTU for the correct port setting to ensure communication between the software and the DAU, and also to set the clock in the DAU to the PC's system time. Once this is done, you can begin to program the tours into the software.

Let's assume that a tour has 20 checkpoints, including the start point. The simplest way to set up the tour is to lay out on a table or desk 20 data points (magnetic strips or RFID tags) and to number them from 1 to 20 (with a piece of masking tape, for example). The list of checkpoints for that tour should also be numbered in order from 1 to 20, beginning with "1" for the start point.

With a cleared DAU (no data in the memory), read the 20 data points in order from 1 to 20. Then download the 20 data point readings into the software. The procedures for assigning the data points to a tour vary, depending on the software; In WinArgus, for example, the 20 downloaded data point readings must be converted to a "master file" that contains the tour. In TopGuard Patrol, the 20 data point readings go into a "pool" from which they are selected and assigned to a tour. Check the software's documentation for the appropriate procedures.

Once the 20 data points are assigned to a tour, the description for each checkpoint from the client's list is typed into the software for each data point. The name of the tour is also typed into the software. Once this is done, the programming of the tour is complete. The 20 data points should be collected and installed in their respective locations, based on their identifying numbers and referring to the client's tour list.

This process should be repeated for each tour on the client's list. Care should be taken in the labeling and handling of the data points to avoid confusion about which data point is to be mounted in which location.

This is particularly true if some data points are to belong to more than one tour. With the WinArgus software, it is necessary in this case to actually read such data points each time they are programmed into a subsequent tour. With the TopGuard Patrol software, once the data points are read and downloaded into the "pool," it is not necessary to read them again in order to assign

them to multiple tours; they can just be selected from the pool and assigned to as many tours as desired.

Ideally, the guard tour system is set up prior to installing the checkpoints at their eventual physical locations. It is easier to read the data points altogether in one place and download them than it is to physically walk the tour, recording each data point and its location, and trying not to get them confused.

The incident strips/tags and officer identification data points are basically programmed into the software the same way. The ProxiPen incident books all contain the same set of 12 RFID tags, thus it is only necessary to program them into the software once. The same is true for the Escorte incident books, except that books are available with additional sets of 20 incident strips (21-40, 41-60, etc.).

Installing the Checkpoints

The data points that have been programmed as checkpoints on a tour should, insofar as possible, be mounted in locations that are out of the weather and direct sunlight; this will prolong their useful life. This being said, the data points are readable even when wet, frosty, covered with dirt, grease or grime or having been painted over. They should also be mounted where they are least visible but still readily accessible to the officer; this will prevent damage and vandalism to the data points. For example, data points can be mounted on a doorjamb – preferably on the hinged side – where they are not visible until the door is opened.

The data points should not be mounted where an electromagnetic field may be present, such as on a motor, transformer or fluorescent light fixture. The magnetic field will not damage the data point, but attempting to read the data point may result in garbled data and a corrupted download file.

The Escorte magnetic data strips are surface mounted. The adhesive-backed data strip comes with a strip of extremely strong, double-sided adhesive tape on its back; peel off the protective cover and apply the strip to any relatively flat, nonporous surface. The metal-backed data strip and the Mega Strip can be mounted with either regular or non-reversing screws.

The ProxiPen RFID tags have the advantage that they can be read without contact from a distance of up to $\frac{3}{4}$ " , depending on the strength of the ProxiPen's battery. Because they are read via proximity, they can be either surface-mounted or concealed behind any nonmetallic material: glass, mirrors, wallboard, paneling, stucco, etc. This can be helpful where aesthetics, vandalism, etc. are considerations.

Insofar as possible, the ProxiPen RFID tags should not be mounted directly on metallic surfaces (especially ferrous metal), as such surfaces interfere with the radio signal transmission/reception process by which the ProxiPen reads the tags. If the RFID tags must be mounted on such surfaces, a spacer should be mounted between the tag and the metal surface. The spacer can be made of any nonmetallic material (i.e., plastic, wood, plexiglass, rubber, etc.) and should be at least the same thickness as the tag. Spacers are available from Detex, but the end user may choose to obtain spacers elsewhere or fabricate them himself.

The data points should be mounted in locations where the officer is compelled to perform the desired task in order to read them. For example, if there is a large room that should be examined completely by an officer, mount the data point at the far side of the room so that the officer must

observe the entire room while walking to the data point's location. Or, if the officer is to read a gauge and verify some operational parameter, mount the data point so that the officer can't help but see the gauge while reading the data point; on the side of the gauge, for example.

Copy Protection Devices

If the client has purchased software that requires that a copy protection device (dongle, key, etc.) be attached to the PC in order for the software to operate, you cannot overstate to the client the importance of not misplacing that device. It is effectively what they are paying for when they purchase the software; Detex will replace diskettes, CD-ROM's, or manuals at little or no cost to the client, but if they misplace the copy protection device, they must essentially buy the software all over again.

And this happens more often than one might think. A client will purchase new computers for their business and arrange to have the vendor come in during an evening or weekend to replace them, not giving a thought to the dongle hidden on the back of one of the machines. The vendor takes the old machines away and the copy protection device usually disappears.

It is a good idea for the distributor to give the client a letter stating these points to the client at the time of purchase and to keep a copy of the letter in his files. The letter may or may not help the client to remember the copy protection device, but it certainly makes matters more comfortable for the distributor, and for Detex, in the event that the dongle is eventually misplaced.