

# AXIS Diplomat

## Technical White Paper

### **Data Security Best Practice**

#### **1. Introduction**

For the majority of our customers, AXIS Diplomat lies at the heart of their business and any “down-time” during working hours or loss of data is a business critical issue. This document discusses some of the causes of data loss or downtime which are outside of the control of AXIS First.

The causes for these incidents include

- Inadequate backup frequency.
- Insufficient backup copies (e.g. using the same single backup media every day).
- Failing to check backup logs (and finding out too late that errors have been occurring).
- Using backup software which is either not up to the job, badly installed or incorrectly configured.
- Infection and attack by virus software.
- Bugs in third party products.

#### **2. AXIS Diplomat Data Security Developments**

##### **2.1 Multiple & Automatic Checkpoints**

These are extensions to AXIS Diplomat’s long-established data protection facilities. Previous facilities relied on operators running a “checkpoint” function periodically to declare the system “clean”, to which the system could be rolled-back to in the event of a failure.

AXIS Diplomat automatically attempts to take a checkpoint whenever data has been entered. In the event of a system failure a checkpoint represents a “clean” point to which the system can be rolled back. Where the system is not at a clean point (for example because another operator is in the middle of filing a batch of data), and a checkpoint cannot be taken, the system simply continues. The next time an operator completes an update, the system will try again, and so on. Manual checkpoints can also be taken before.

AXIS Diplomat holds many checkpoints (typically hundreds), allowing the operator to select the point to which to roll-back to (usually the most recent).

##### **2.2 Secure Systems**

Most server-based operating system environments (such as Microsoft Windows Server) provide the ability to restrict access to files on disk according to the current logged-in user.

AXIS Diplomat utilises the security access rights assigned to Windows user accounts and group to restrict access to the AXIS Diplomat files (both programs

and data). This can severely limit the damage that virus software can do to your AXIS Diplomat system in the event of an infection since the virus will not be able to access key AXIS Diplomat files.

### **2.3 AXIS Diplomat Backup Facilities**

AXIS Diplomat has build-in backup facilities which offer the following features:

- Multiple backups can be stored on your hard disk. Specific backups (such as month end backups for example) can be flagged as being retained indefinitely on the hard disk.
- Backups are compressed. Compression technology means that the disk space required for an AXIS Diplomat backup is minimised. As well as allowing multiple backups to be archived on the hard disk of the server, this allows you to take advantage of removable media such as memory sticks.
- Backups can be automated. You can schedule a backup to happen automatically at a given time, at given intervals. For example, you could schedule an automatic backup to happen at 23:00 on every week day.
- Backups can include all the parameter and miscellaneous files associated with your AXIS Diplomat system, not just the transactional database. This means that your system can be rebuilt precisely as it was before with just the backup file and your most recent AXIS Diplomat release software.
- The backup facilities works in conjunction with the AXIS Diplomat SoS service (Safe off-site Storage) to automatically backup your AXIS Diplomat system to our web servers providing further peace of mind that your day's data is protected and providing an important element in your business' disaster recovery plan.
- Backups can be transmitted via the internet to AXIS First ad-hoc. This allows our support team to investigate any support query "off-line" without affecting the operation of your live system.
- Two-phase backup reduces the time during which users can not access the system. During the first phase, the data is copied and, as soon as that has been done, users are allowed to continue updating the system. The backup function is then able to compress the copied data without time constraints (by being able to spend more time on the compression phase, the resultant backup file can be as small as possible). This achieves the best of both worlds where, as far as the users on the system are concerned, the backup happens very quickly but also the backup file is extremely compact.
- New "Waiting for Supervisor Mode" operation waits for other operators to exit the system whilst preventing new users signing on until the first backup phase has been completed.

### **2.4 Safe Off-site Storage ("SOS")**

SOS is a subscription-based service whereby the AXIS Diplomat backup function can automatically transfer the backup to AXIS First's secure servers. The three most recent backups are retained on those servers. Software running on those servers monitors arrivals of backups from each subscriber and raises an alert if backups are not received, or are incomplete.

Storing your most recent AXIS Diplomat backups off-site provides you with the best security of that data since, even if your building or network is destroyed by fire or flood, the data is safe. The backups stored on our servers are also backed up on a daily basis and stored off-site so, even assuming the worst case scenario of both the AXIS First offices and your offices being destroyed simultaneously by fire, we would still have an off-site backup of your data!

### **3. Data Security Best Practice**

#### **3.1 Data Protection**

The Data Protection facilities within AXIS Diplomat (sometimes referred to as "checkpointing") should be your first line of defence against data protection. Using the standard facilities for multiple and automatic checkpoints, data loss as a result of a system crash can usually be minimised to a few minutes.

#### **3.2 Tape or removable media backups**

No data protection facilities should be considered as a replacement for backups to tape or other removable media which can be rotated off-site. All systems should be backed up to removable media on a daily basis (normally automated overnight) and you should have a defined procedure for media rotations. These backups are your main defence against system loss – if, for example, your server suffers a catastrophic hardware failure, is stolen or otherwise lost, these backups are the first port of call.

Your backup software should include the following facilities:

- Disaster Recovery (DR) – without Disaster Recovery (or "bare metal" disaster recovery) in order to restore a backup, it is necessary to rebuild a complete server first, then install the backup software to read the backup – this could, in extreme cases, involve several days of work for a systems software engineer, before being able to restore!
- Open File Backups – on Windows systems, and servers in particular, many of the Windows system files are open all of the time and, without a mechanism for backing up those open files, you cannot restore a complete system, only the parts of the system that were not open at the time (and an incomplete backup can be as bad as no backup at all!).

A typical media rotation scheme for tape is as follows:

Starting with twenty tapes, rotate each tape on a daily basis so that you have a Monday tape that is used once every four weeks, a Tuesday tape, and so on. At the end of each month, take out the tape for the last day of the month and archive as a month end tape and replace that tape with a new one. This helps ensure that you have, not only the backups for the last four working weeks but also an archive of backups from each month end. Furthermore, by introducing a new tape into the cycle at each month end, you are avoiding making backups onto the same tape over and over again – like VHS tapes, data cartridges have a finite life span, and you may not find a problem until you try to restore the tape.

You should always perform a full system backup, and not an incremental backup. Incremental backups only backup the data that has changed since the previous backup and so piecing a system back together can require multiple tapes, which is problematic at best.

You should also ensure that every tape backup includes a verify operation. This is when the software reads back the contents of the tape and compares with the files that have been backed up to ensure that the backup is complete and correct.

Avoiding incremental backups, and including a verification pass, will increase the time taken for a backup and, for this reason, we recommend that tape backups are scheduled for overnight execution, when the time taken for the backup is largely irrelevant.

You should also endeavour to store your backups off-site (by sending the most recent backup home with a responsible employee, for example). Ensure that tapes are brought back in before they are next required in the rotation. When not off-site, tapes should be stored in a secure location, such as a fireproof safe.

### **3.3 AXIS Diplomat Backups**

You should schedule an AXIS Diplomat backup overnight prior to the removable media backup – that backup then includes the AXIS Diplomat backup file in addition to all of the files associated with the AXIS Diplomat system – this makes it much easier to restore a system since you can reload that one backup file in the event of a failure.

AXIS backups can be archived to removable media such as external disk drives, memory sticks or DVDRW drives.

### **3.4 Secure Systems**

If you are running your AXIS Diplomat system on a server that supports security (e.g. Microsoft Windows Server) you should install the Security Option to help protect your system from malicious attack by viruses, hackers, etc. and accidental damage by users inadvertently trying to delete the wrong file.

### **3.5 Safe Off-site Storage (“SOS”)**

Provided that you have a suitable Internet connection, the SOS service provides the best mechanism for securing your AXIS Diplomat data off-site. Your backups are stored off-site immediately because they are uploaded automatically via the Internet; with normal off-site regimes, the tape may not go offsite until the end of the following day – if your server gets stolen overnight, it makes no difference whether the tape backup succeeded or failed since the tape was inevitably stolen along with the server anyway!

## **4. Conclusion**

Whilst there may, on the surface, seem a thin line between Data Security Best Practice and paranoia, you should consider your procedures carefully. Data is virtually uninsurable and a significant loss of data often results in a business failure. Consider, for example, the scenario of fire destroying your offices. Your insurance company will (hopefully) replace the building and your IT systems but, with any paper records destroyed, the data held in the AXIS Diplomat system is the only place you will find a record of who owes you money, who you need to fulfil orders for and, indeed, who your customers and suppliers are!