ATTENDANCE VERIFICATION SYSTEM POLICY AND GUIDELINES

Research and Personnel Systems Directorate
People and Standards Division

Foreword

The following document has been prepared as an aid to those Ministries/Departments/Entities intending to introduce an automated Attendance Verification System (AVS) for the purpose of security, recording attendance, salary computation and audit trails. The document is aiming to serve as a guideline and outline policies and not to favour any particular system/device. Line Ministries/Departments/Entities should be aware of their responsibilities under Data Protection Legislation and to the sensitivity of the privacy of their employees. Data Protection Guidelines in relation to Attendance Verification Systems should also be referred to.

Contents

01

Introduction

1.   Introduction

Attendance verification devices, together with their accompanying software, help eradicate fraud, reduce time wasting and provide more effective use of human resources. This technology is an effective means of capturing attendances and absences of employees in the Public Service by means of decentralised external and internal electronic reading devices and inserting them automatically into the relative HR system. It also eliminates lengthy manual data entry of absences from attendance sheets and Muster rolls into the system.

These systems are intended to reduce to a minimum manual process in the recording of attendances and absences, while ensuring that they are accurately recorded in real time, and the necessary adjustments made in the relative HR systems. These devices, while observing good Data Protection practices, and without threatening the employees' fundamental rights and freedoms, help Government Departments and Entities get what they are paying for in salaries.

02

Identification Devices and Biometric Data

2. Identification Devices and Biometric Data

2.1 Types of Access & Identification Devices

AVSs are primarily used to authenticate and keep record of the time of entry and exit of employees, manage absences, and to automate the initial part of the payroll process. These use various types of Access and Identification Devices such as:

- Conventional Recognition Devices (CRD): these devices include swipe cards, electronic tags, smart cards, punch clocks and others.
- Biometric Recognition Devices (BRD): these devices include voice, face geometry, fingerprint, iris scanning and hand/palm recognition'

All biometric systems operate on the basis of the automatic identification or authentication/verification of a person. What differs between the systems is the nature of the biometric data and the type of storage.

2.2 Conventional Recognition Devices

These devices, although electronic in nature, may take different forms and may contain such elements as bar coding, magnetic tapes, static memory and other electronic media.

2.3 Biometric Recognition Devices

Biometric data may be created from physical or physiological characteristics of a person. These include a fingerprint, an iris, a retina, a face, outline of a hand, voice pattern, and DNA. Biometric data might also be created from behavioural data such as handwriting or keystroke analysis. Generally, a digitised template is produced from the biometric data. This template is then compared with the one produced when an employee uses the reader.

2.3.1 Biometric Identification

Biometric identification confirms the identity of an individual by comparing a 'biometric signature' to all records stored in a database to determine if a match exists. If there is a match, the identification is successful. Since it requires comparing each existing record in the database against the new biometric characteristic, it can be slow if the database is large. This category is less commonly used for real-time applications such as access control or time and attendance.

2.3.2 Biometric Authentication/Verification

Authentication/verification systems confirm that the biometric data derived from a person who presents an image at a reader matches another typically stored on a card and presented simultaneously. The biometric feature will only be compared to the one previously saved individual's biometric 'signature'. If there is a match, authentication/verification is successful. This is usually done by storing the biometric image against a numeric identifier. Every person is requested to enter his/her unique identifier when clocking in and out and the system compares a recent file stored against the signature presented. Thus, clocking will be accomplished much faster, and the level of accuracy of the machine can then be lowered.

2.4   Biometric Authentication/Verification

There are three principal types of biometric data

- Raw Images: these consist of recognisable data, such as an image of a face or a fingerprint, etc.
- Encrypted images: these consist of data that can be used to generate an image.
- Encrypted partial data: these consist of partial data from an image, which is encrypted and cannot be used to recreate the complete original image.

It is this office's policy that in order to ensure good data protection practices, any AVS installed in any Ministry should be of the third type, i.e. Encrypted Partial Data.

2.5   Storage of Biometric Data

There are two principal methods of storing biometric data/templates:

- Central databases: these store the templates on a central system which is then searched each time a person presents his/her biometric image at a reader.
- A card is used to store a template. A template is generated when a person presents his/her biometric image at a reader, and this template is compared with the template on the card.

03

Data Protection issues concerning Biometrics

3. Data Protection issues concerning Biometrics

When considering the introduction of an AVS, the Data Protection Legislation should always be adhered to. Particular emphasis is being given to the following points:

a) personal data is processed fairly and lawfully;
b) personal data is always processed in accordance with good practice;
c) personal data is only collected for specific, explicitly stated and legitimate purposes;
d) personal data is not processed for any purpose that is incompatible with that for which the information is collected;
e) personal data that is processed is adequate and relevant in relation to the purposes of the processing;
f) no more personal data is processed than is necessary having regard to the purposes of the processing;
g) personal data that is processed is correct and, if necessary, up to date;
h) all reasonable measures are taken to complete, correct, block or erase data to the extent that such data is incomplete or incorrect, having regard to the purposes for which they are processed;
i) personal data is not kept for a period longer than is necessary, having regard to the purposes for which they are processed.

Detailed Data Protection requirements for Attendance Verification Systems (AVSs) can be found on the Intranet under Data Protection Guidelines in the Data Protection Section.

04

Systems Administration

4. Systems Administration

The Ministry's Chief Information Officer (CIO) shall be the Central Systems Coordinator. The Director Corporate Services (DCS) shall assist the CIO with the Administration of data on such matters. In cases of outstations, the CIO and DCS should co-ordinate with the Head of Department to tackle any issues that may arise.

The Department's Data Protection Officer (DPO) should be consulted at all times – prior to selecting the preferred type of device, during installation, during initial data collection, and after implementation. At this stage, advice form the DPO should be sought in the compilation of a Data Protection Impact Assessment. The DPO should also be the contact point for any Data Protection issues between the Ministry's CIO and DCS, and the Data Protection Commissioner.

The Ministry's CIO, in conjunction with the DCS, shall carry out regular inspection/maintenance of the recognition devices. Planned maintenance should be carried out outside normal office hours so as to avoid disruptions to the employees within the Ministry/Department/Entity.

05

Security

5.   Security

The Ministry/Department/Entity shall have appropriate security measures in place to prevent unauthorised access to, or the unauthorised alteration, disclosure or destruction of data. Technological solutions such as encryption are recommended.

5.1   Standard of Security

A minimum standard of security would include:

- Access to the information restricted to authorised staff on a 'need to know' basis in accordance with a defined policy;
- Computer systems should be password protected;
- Information on computer screens or manual files should be hidden from persons who are not authorised to see them;
- A back-up procedure for computer held data, including off-site back-up;
- Ensuring that staff are made aware of the workplace's security measures, and comply with them;
- Careful disposal of documents such as computer printouts, etc.;
- The designation of a person with responsibility for security and the periodic review of the security measures and practices in place;
- Adequate overall security of the premises when it is unoccupied;
- Where the processing of personal data is carried out by a data processor on behalf of the employer, a contract should be in place which imposes equivalent security obligations on the data processor.

5.2   Retention Policy

The Data Protection Legislation provides that data shall not be kept for longer than is necessary for the purpose. In the context of a biometric system in a workplace, it would be necessary to devise a retention policy in advance of the deployment of the system which clearly sets out the retention period which would apply to biometric data. It is expected that as soon as an employee permanently terminates his/her employment at the Ministry/Department/Entity, his/her biometric data would be immediately deleted.

Access by Guests/Visitors And Fallback Procedures

6. Access by Guests/Visitors and Fallback Procedures

Wherever the Access and Identification Device is used also as a device to control and monitor access to the Ministry/Department/Entity, a formal procedure must be in place for access by anyone who is not registered in the system.

This may include the use of Visitor/Guest Cards or Tags. It is recommendable that appropriate registers be kept in relation to this matter. The same procedure shall be used for any officer who has not been identified by the system, misplaced/lost/forgotten his recognition tag/card (pending the issue of a replacement card), etc.

The procedure shall also include details regarding by whom guests/visitors are to be accompanied and escorted to the offices (messenger/security guard/etc.).

6.1 After Office Hours/ Weekends / Public Holidays

Visitors/Guests should not be allowed in the premises outside normal office hours, during weekend and Public Holidays without the Director/Head of Department/ Manager's prior consent. Devices can also be set to restrict the time employees or certain categories of employees can be allowed to use the devices in order to eliminate early 'in' punches and unauthorised overtime punches. If an employee attempts to use the system during an unauthorised time, the system will display 'time restriction'.

6.2 Terminations / Transfers

The Systems Administrator shall ensure that, whenever any officer is transferred to another department, retires, is medically boarded out, is dismissed, or his employment is terminated in any other way, any card/tag is collected back from such officer and deactivated, the officer has no longer access to the premises and that the officer's biometric data is deleted from the system.

6.3 Reporting Lost Cards/Tags

Wherever the Recognition Device uses also a Card/Tag, an appropriate procedure should be in place for reporting misplaced/lost Cards/Tags to the Office of the DCS. Pending the issue of a new Card/Tag, officers who have misplaced/lost their Access Card/Tag shall be issued with a Temporary Visitor/Guest Card. The misplaced/lost card should be cancelled so that anyone finding such a card would not be able to access anywhere with it.

6.4 Non-office bound workers / Duty outside department's premises

Where the Ministry/Department/Entity employs workers, who are not office-bound, appropriate equipment shall be procured for such workers. These can include portable devices which shall be fully integrated into the central system. When such portable devices are used, supervisors should ensure that clocking is actually taking place in or near the place it is intended, and not from some other place. When it is found that persons are clocking from other places, proper disciplinary measures against the individual/s should be taken. If it will be difficult to establish the true clocking place, necessary arrangements should be made so that these employees' clock in the nearest Local Council Office or from some other place equipped with devices attached to the central system.

Furthermore, proper systems shall be put in place for the recoding of duty outside the Ministry/Department/Entity's premises, duty overseas etc.

6.5 Fallback Procedures

Since recognition devices are not completely accurate, readily available fallback procedures should be developed and implemented in order to respect the dignity of persons who could not provide readable fingerprints or could have been wrongly identified/unidentified by the system and to avoid transferring onto them the burden of the system's imperfections.

6.6 Attendance Sheets

When attendances of every person whose name appears on the department's manual Attendance Sheets are captured electronically, the function of the signed forms is no longer valid. Every supervisor must ensure that by the end of every working day, absences of all persons under his/her charge are all accounted for that particular day, and a complete print-out of the persons' attendances/absences for that particular day can be made on demand.

General Considerations

7.   General Considerations

- All types of biometric data should be of the type that could not be reverse engineered to identify the individual. It should not store the image (of the hand fingerprint etc.), but should store, instead, a mathematical representation of the image. This mathematical value is meaningless to other devices. In addition, no fingerprint or palm print information should be extractable from the system.
- AVSs should be invariably installed in every entry or exit point within the premises, and the number of units should be dictated by the number of persons present in the respective premises at any given time. Premises with more than one entry or exit point should be altered in such a way as to channel employees through entry and exit points where the devices are installed. Entry and exit points which do not have devices should be blocked, but keeping in mind that, in the case of a fire or any emergency, they can be re-opened and employees re-channelled through.
- Persons should not be penalised for clocking-in late because of an insufficient number of devices, and it should be ascertained that sufficient devices are available, according to the number of persons working in the premises.
- A clock attached to the device, clearly showing the real time of the clocking device, should be clearly visible by the persons using the device. If more than one clocking device is used, clocks and clocking devices should be interconnected showing the same time.
- All persons, irrespective of grade, rank and position, should use the clocking devices, and they should invariably clock-in and clock-out every time they enter or leave the premises, being for breaks, official business or any authorised/unauthorised absences. Persons who fail to use or willingly try to avoid using this facility or try to misguide the clocking device in some way or other, will be liable to disciplinary proceedings.
- The software of the clocking devices should allow authorised users to approve timesheets up to a pre-determined time daily and give details of absences of employees under his/her responsibility. Planned absences, like vacation leave, maternity leave, etc. should be set up on the system's calendar in advance by the supervisor.
- There may be instances where different types of clocking devices will be required for different sites, and different devices for the same sites according to the specific requirements of departments/ministries. The respective Permanent Secretary, in collaboration with the Ministry's Chief Information Officer (CIO) and DPO shall decide which type of approved clocking devices are most suitable for the specific requirements of the sites within the respective Ministry.
- AVSs are sensitive and expensive electronic devices. Sufficient precautionary measures should be taken to prevent accidental or voluntary damage in each and every site where these devices are in use, especially in outstations. When such damage is witnessed or proved, the necessary disciplinary measures are to be taken.