GPA ID Pass Scheme

Guidance for Nominated Officers & Authorised Signatories V3.0

ABBREVIATIONS

AC	Accreditation Check (National Security Vetting Level)
AIC	Airport Identity Card
APHIDS	Access Pass Holder Information Distribution System
AS	Authorised Signatory
ASAT	Airside Safety Awareness Training
CAA	Civil Aviation Authority
CRC	Criminal Records Check
CTC	Counter Terrorism Check (National Security Vetting Level)
DfT	Department for Transport
DV	Developed Vetting (National Security Vetting Level)
GPA	Glasgow Prestwick Airport
GSAT	General Security Awareness Training
HMRC	Her Majesty's Revenue & Customs
ID	Identity
NO	Nominated Officer
NSV	National Security Vetting
UK	United Kingdom
SC	Security Check (National Security Vetting Level)
SeMS	Security Management System
SRA	Security Restricted Area
TEP	Temporary Employment Pass
TVP	Temporary Visitor Pass

Link to Contents

1 INTRODUCTION

This Guidance sets out the standard requirements of the Glasgow Prestwick Airport (GPA) ID Pass Scheme for all Nominated Officers and Authorised Signatories approved by GPA. This Guidance should also be read in conjunction with the GPA ID Pass Scheme Terms & Conditions.

The standards requirements guard against the threat from insiders, and pass holders exploiting their credentials to commit acts of unlawful interference against Civil Aviation. This may manifest itself in an individual attempting to obtain an Airport Identity Card (AIC) or Temporary Pass by fraudulent application, using deliberate deception.

Adherence to this Guidance is important to safe guard the integrity of the Scheme and to ensure that only properly vetted and suitable candidates are issued with an GPA AIC, Temporary Visitor Pass (TVP) or Temporary Employment Pass (TEP) and that ALL individuals working in an airport environment exude the fundamental standards of general security awareness, namely:

- Trustworthiness
- Reliability
- Integrity
- Safety and Security minded; and
- Situationally aware of the current threats to aviation

This Guidance has also been created in line with the Department for Transport (DfT) Airside Pass Scheme Guidance to ensure compliance with our regulatory responsibilities. It also forms part of our regulated Airport Security Programme measures relating to insider threat, raising staff awareness and promoting a security culture.

Companies and Participant organisations who require Glasgow Prestwick Airport to issue an AIC or Temporary Pass to their employees or representatives are required to appoint a Senior Leader or Executive to assume the role of Nominated Officer (NO). This NO is accountable for ensuring the Terms and Conditions of the GPA Airside Pass Scheme are met.

The NO can then appoint Authorised Signatories (AS) who should be focused on the accurate delivery of all pass applicants background checks and training requirements to the standard detailed in this Guidance.

GPA endorses a Security Management System (SeMS) culture which puts Safety and Security at the heart of the participant organisation. Nominated Officers and Authorised Signatories are expected to embody the GPA SeMS philosophy.

2 JOINING THE GPA ID PASS SCHEME

Any company or participant organisation (therein referred to as 'participant organisation' in this guidance) requiring Glasgow Prestwick Airport (GPA) to issue an Airport Identity Card (AIC) or Temporary Pass to their employees or representatives (therein referred to as 'employee' in this guidance) must join the GPA Airside Pass Scheme (therein referred to as 'the Scheme' in this guidance).

GPA will conduct checks on the participant organisation before accepting registration on the Scheme. This is to verify that:

- it is a legitimate business; and
- it can prove a business/ operational need for having its employees accessing the appropriate areas of GPA

Notwithstanding, a commitment to meet the Scheme Terms & Conditions is pursuant to:

- the appointment of a Nominated Officer (NO) to act as the accountable person to GPA; and
- an obligation to assure itself of the suitability and the integrity of its AIC/Temp Pass applicants; and
- providing ongoing assurance that Authorised Signatories (ASs) and individuals working at GPA (employees and contractors) maintain the fundamental standards of:
    - Trustworthiness, Reliability and Integrity
    - Safety and Security minded; and
    - Situationally aware of the current threats to aviation

2.1 Prior to Joining the Scheme

All participant organisations must be supported by a written letter of justification and one of the following:

- a copy of a legal contract with GPA or another participant organisation operating at the airport; or
- evidence that the participant organisation is undertaking a regulated aviation security or other statutory activity

Financial and other checks will be carried out on any participant organisation applying to join the Scheme. The purpose of these checks is to determine that the participant organisation is a legitimate ongoing business concern with a genuine reason for employees to have an AIC or Temp Pass.

Participant organisations must sign a legal agreement confirming adherence to the Scheme Terms & Conditions.

2.2 Applying to Join the Scheme

All participant organisations who want to join the GPA ID Pass Scheme must read the GPA ID Pass Scheme Terms & Conditions, complete and sign Appendix 2 and send to the GPA Security ID Unit.

Expressions of interest to join the Scheme or any questions can also be made via email to: securityidunit@glasgowprestwick.com

2.3 Payment of Charges

Participant organisations will be required to state in Appendix 2 (of the GPA ID Pass Scheme Terms & Conditions) how charges will be paid. The preferred method of payment is credit/debit card at the point of delivery. This can be an applicant's credit/debit card or the participant organisation's credit/debit card. Card payments can be made over the telephone. Cash payments cannot be accepted. Alternatively, a participant organisation can apply to GPA to pay in arrears by invoice. GPA will carry out due diligence before approving invoice payments and always reserves the right to require payment at the point of delivery.

3 THE NOMINATED OFFICER (NO)

On joining the Scheme every participant organisation must appoint a Nominated Officer (NO), who should be a Senior Leader or Executive with the authority to allocate the necessary resources required to meet the standard requirements of the GPA ID Pass Scheme. A NO is required for each participant organisation; however, a caveat exists for the appointment of a separate NO for subsidiaries. The NO will determine and appoint the appropriate number of Authorised Signatories (ASs) and be accountable for ensuring that they discharge their responsibilities.

3.1 Requirements of the Nominated Officer (NO)

The NO shall:

- have full accountability for meeting the participant organisations obligations under the Scheme; and
- have sufficient authority for assuring the participant organisations employment screening policies and procedures; and
- understand the risks associated with insiders and the importance of risk mitigation measures; and
- have the authority to require the removal of an AIC or Temp Pass from any employee who is no longer considered suitable to hold it

The obligations of the NO are:

- to appoint and oversee the work of all ASs, putting the appropriate training and Quality Assurance Systems in place, to uncover possible fraudulent, unlawful or negligent activities. In a small participant organisation, the NO Officer can also be the AS; and
- to demonstrate visible leadership on security issues, ensuring that AIC holders and ASs are briefed on their responsibilities; and
- to work with other senior colleagues within the participant organisation to ensure that AICs are managed responsibly and returned to GPA when no longer required; and
- to communicate the requirements of the Scheme (alongside any changes) to Senior Management and ensure implementation of any resulting changes needed to participant organisation policy or action; and
- to ensure that any investigations, audits or inspections undertaken by GPA receive full cooperation, and that any identified deficiencies or need for additional controls are actioned; and
- to alert GPA when an AIC or Temp Pass is either compromised or no longer required by an individual and, if appropriate, alerting the authorities where fraudulent or criminal activity is suspected or uncovered

In addition, the NO must:

- normally attend a face-to-face Security Interview with GPA – this can be done virtually if required
- conduct a Security Interview with all Authorised Signatories using Form IDPS 02 – Authorised Signatory Interview & Declaration

3.2 Nominated Officer (NO) Entrance Interview

All NOs will normally need to attend an entrance interview at the GPA Security ID Unit prior to their participant organisation being accepted onto the Scheme. The purpose of the entrance interview is to:

- better understand the nature of the participant organisation's business and operation at GPA; and
- ensure that they understand the expectations and obligations of the NO function; and
- ensure a full understanding of the insider risk coupled with an assurance that ASs perform their task responsibilities inclusive of personnel security and pass management to include an annual review of all active AIC holders; and
- confirm GPA's right to suspend/withdraw any individual's AIC or Temp Pass and to suspend/withdraw the participant organisation's membership of the Scheme as detailed in the Terms & Conditions.

4 THE AUTHORISED SIGNATORY (AS)

The Authorised Signatory (AS) performs a vital role in the Scheme. The AS must be based in the United Kingdom and must be directly employed by the participant organisation. The function of an AS is to sponsor AIC applications for their participant organisation. This means they will confirm to GPA that each applicant has a legitimate business need to hold an AIC or Temp Pass and, having successfully completed the appropriate background check to the standard required, approve the applicant as a suitable AIC holder.

4.1 Requirements of the Authorised Signatory (AS)

The AS is a responsible role requiring the following key skills and attributes:

- Excellent participant organisational skills; and
- Attention to detail; and
- Sound judgement; and
- The highest standards of integrity

The AS is responsible for:

- ensuring that the appropriate background check conducted on an applicant is done to an exemplary standard in accordance with GPA standards; and
- sponsoring and approving a pass application only when satisfied the applicant is a suitable candidate to hold an AIC; and
- establishing an applicant's legitimate need for an AIC and providing an indication of the appropriate access level to the decision maker at GPA; and
- alerting the Nominated Officer (NO) to any signs of suspicious or fraudulent activity; and
- co-operating with any requests for information from GPA in relation to applicants and existing AIC holders, and with investigations, audits or inspections undertaken by suitably qualified GPA Security Staff

4.2 Delegating Elements of the Background Check

The AS may delegate or sub-contact tasks associated with the appropriate background check to another person or third party (e.g., the obtaining of a reference or holding a security interview with the applicant) however, the participant organisation registered on the Scheme retains accountability for any elements that are sub-contracted. This means the NO retains overall accountability for any sub-contracted services.

For this reason, the AS must maintain oversight of the sub-contacted parties and be satisfied that all requirements have been met in full. This includes being satisfied that the procedures used mitigate the risks of deception both by the AIC or Temp Pass applicants and the individual(s) completing the checks. A Quality Assurance Framework and Service Level Agreement should be considered as part of any contract for service.

4.3 Applying to be an Authorised Signatory (AS)

Once your participant organisation has been registered on the Scheme, your NO will appoint and sponsor direct employees to act as ASs. In small participant organisations the NO may also be the AS.

Applications to become an AS can only be made via the participant organisation registered on the Scheme. An AS must:

- currently hold a valid GPA AIC; **or**
- have successfully completed an appropriate background check (this must be initiated and conducted by GPA); and
- attend a Security Interview with the Nominated Officer

4.4 Authorised Signatory (AO) Entrance Interview

All ASs will need to attend an entrance interview with the Nominated Officer (NO) prior to approval by GPA. The purpose of the entrance interview is to:

- ensure that they understand the expectations and obligations of the AS function; and
- ensure a full understanding of the insider risk coupled with an assurance that they will perform their task responsibilities inclusive of personnel security and pass management which will include an annual review of all active AIC holders; and
- confirm GPA's right to suspend/withdraw any individual's AIC or Temp Pass and to suspend/withdraw the participant organisation's membership of the Scheme as detailed in the Terms & Conditions.

Form IDPS 02 – Authorised Signatory Interview & Declaration should be used by the Nominated Officer during the interview

4.5 Appointment of Authorised Signatory (AS)

The NO should send the completed Form IDPS 02 – Authorised Signatory Interview & Declaration to the GPA Security ID Unit for registering of the appointed AS. This form can be e-mailed to securityidunit@glasgowprestwick.com

Once appointed, an AS must approve and submit all AIC or Temp Pass applications for anyone:

- employed by your participant organisation; and/or
- sub-contracted to work for your participant organisation

5 SELECTING THE RIGHT AIC or TEMPORARY PASS

The GPA Security ID Unit issues two types of Airport Identify Cards (AICs) under the Scheme – Airside (non-SRA) and Airside (SRA). In addition, they must issue any Temporary Visitor or Employment Passes when access is required to the Security Restricted Area (SRA) and/or any works are being carried out in an airside tenanted building and/or on an apron/taxiway .

A map showing the GPA Security Restricted Area (SRA) can be found at Annex 1 to this guidance

5.1 Airside (non-SRA) Airport Identity Card

This type of AIC is a photo card and is only appropriate to those employees who require on-going landside and/or airside access that does NOT include the SRA.

It is issued for a period not exceeding 3-years; however, this may be shortened where:

- the applicant has temporary right to remain in the United Kingdom; or
- where the participant organisation contract or tenant duration at GPA is less than 3 years; or
- where the applicant or participant organisation no longer meet the requirements detailed in the Scheme Terms & Conditions

Vetting & Training Requirements:

- An initial face-to-face Security Interview is conducted by the AS – see Part 6
- Standard Background Check completed by the AS - see Part 7
- On-going review via the Access Pass Holder Information Distribution System – see Part 9
- Applicant successfully completes General Security Awareness Training (GSAT) – see Part 11
- Applicant successfully completes Airside Safety Awareness Training (ASAT) – see Part 11

The AS will also need to indicate on the application form which areas are required to be accessible to the applicant. In addition, sufficient justification must be provided as to why access to landside and airside is required. The GPA ID Unit may question the applicants at the time of pass issue to verify that the requested access levels are necessary to the role being undertaken.

5.2 Airside (SRA) Airport Identity Card

This type of AIC is a photo card and is only appropriate to those employees who require on-going landside and/or airside access that INCLUDES the SRA. Any SRA access required will be split down into numbered areas:

Number	SRA Access Area
1	Internal Area (Departure Lounge)
2	Baggage Re-claim Hall
3	Baggage Make-Up Area
4	Ramp
5	Aircraft and their Footprints
6	*Not used by GPA*
7	All areas of the SRA

An AIC (SRA) can be issued for a period not exceeding 5-years; however, this may be shortened where:

- the applicant has temporary right to remain in the United Kingdom; or
- where the participant organisation contract or tenant duration at GPA is less than 3 years; or
- where the applicant or participant organisation no longer meet the requirements detailed in the Scheme Terms & Conditions

Vetting & Training Requirements:

- An initial face-to-face Security Interview is conducted by the AS – see Part 6
- Standard Background Check completed by the AS - see Part 7
- National Security Vetting Accreditation Check including on-going review via the Access Pass Holder Information Distribution System completed by GPA – see Parts 8 & 9
- Applicant successfully completes General Security Awareness Training (GSAT) – see Part 11
- Applicant successfully completes Airside Safety Awareness Training (ASAT) – see Part 11

The AS will need to indicate on the application form which areas are required to be accessible to the applicant. In addition, sufficient justification must be provided as to why access to landside, airside and the SRA is required. The GPA ID Unit may question the applicants at the time of pass issue to verify that the requested access levels are necessary to the role being undertaken.

5.3 Summary of GPA AICs Vetting & Training Requirement

The table below summarises the vetting and training requirements for airside AICs that must be issued by the GPA Security ID Unit:

Type	Mandatory Vetting	Mandatory Training	Renewal Reqd
Airside (non-SRA) AIC	• Face-to-Face Security Interview • Standard Background Check	• GSAT • ASAT	Every 3 Years
Airside (SRA) AIC	• Face-to-Face Security Interview • Enhanced Background Check that includes an Accreditation Check • Ongoing review via APHIDS	• GSAT • ASAT	Every 5 Years

5.4 Temporary Visitor Pass (TVP) - SRA Access Required

This type of temporary pass is only appropriate to a visitor who needs to access the SRA and must be issued by the GPA Security ID Unit.

This paper pass displays the name of the visitor and the name of the trained Escort, who must be a current Airside (SRA) AIC holder and accompany the visitor at all times. One Escort can accompany a maximum of 6 holders of a TVP(SRA). The TVP(SRA) holder must always carry Photo ID (Passport or Photo Driving Licence) at all times.

A TVP (SRA) can be issued for between 1-7 consecutive calendar days. There must be a break of at least 3 calendar days before another TVP (SRA) can be issued to the same visitor.

In addition, in any 12-month rolling period, the same visitor can only be issued with a TVP(SRA) for a maximum of 14 calendar days. Therefore, it is very important the pass is only requested for the exact period required. A part-day counts as a full day.

GPA Security ID Unit Requirements:

- The participant organisation requesting the TVP(SRA) must send completed Form IDPS 06 – TVP Application to the Security ID Unit at least 24 hours beforehand. It can be e-mailed to: securityidunit@glasgowprestwick.com
- The participant organisation must phone the GPA Security ID Unit on 01292 511043 to make an appointment for the issue of the TVP(SRA)
- Both the visitor and designated trained Escort must attend the Security ID Unit at the designated appointment time to collect the TVP(SRA)
- The visitor must provide valid photo ID (Passport or Photo Driving Licence) and carry it with them at all times
- The trained Escort will need to show their Airside (SRA) AIC, confirm they are an approved Escort (and have completed the GPA Escort Training) and fully understand their responsibilities.

The TVP(SRA) must always be returned to the GPA Security ID Unit at the end of the validity period.

All visitors issued with a TVP(SRA) will also be subject to a security review via a weekly upload to the Access Pass Holder Information Distribution System (APHIDS) by GPA – see Part 9.

5.5 Temporary Employment Pass (TEP) – SRA Access Required

This type of temporary pass is only appropriate to a new employee (or sub-contractor) who needs to access the SRA, whilst awaiting the issue of an Airside (SRA) AIC and it must be issued by the GPA Security ID Unit.

This paper pass displays the name of the employee and the name of the trained Escort, who must be a current Airside (SRA) AIC holder and accompany the employee at all times. One Escort can accompany a maximum of 3 holders of a TEP(SRA). The TEP (SRA) holder must always carry Photo ID (Passport or Photo Driving Licence) at all times.

A TEP(SRA) can be issued for between 1-14 consecutive calendar days as long as the employee has no disqualifying convictions and has applied for a Criminal Records Check i.e., Basic Disclosure Certificate.

If a TEP(SRA) applicant has disqualifying convictions, they can apply to the CAA for a Certificate of Disregard – see Part 7.6.

A further TEP(SRA) can be issued for between 15-60 consecutive calendar days but only if the employee has received and provides their Criminal Records Check i.e., Basic Disclosure Certificate.

GPA Security ID Unit Requirements for 1-14 days TEP (SRA):

- The participant organisation requesting the TEP(SRA) must send a completed Form IDPS 07 – TEP Application to the Security ID Unit at least 24 hours beforehand. It can be e-mailed to: securityidunit@glasgowprestwick.com
- The participant organisation must phone the GPA Security ID Unit on 01292 511043 to make an appointment for the issue of the TEP(SRA)
- Both the employee and designated trained Escort must attend the Security ID Unit at the designated appointment time to collect the TEP(SRA)
- The employee must provide valid photo ID (Passport or Photo Driving Licence) and proof they have applied for a Criminal Records Check (CRC) within the past 21-days i.e., UK Basic Disclosure Certificate. A postal or e-receipt is acceptable. If the application has been submitted in paper form only or made by post and there is no application/confirmation number, a copy of the applicant's declaration page will be needed. If the application is submitted via a service such as recorded/special delivery, the tracking number will be needed.

- The trained Escort will need to show their Airside (SRA) AIC, confirm they are an approved Escort (and have completed the GPA Escort Training) and fully understand their responsibilities.

GPA Security ID Unit Requirements for 15-60 days TEP (SRA):

- The participant organisation requesting the TEP(SRA) must send a completed Form IDPS 07 – TEP Application to the Security ID Unit at least 24 hours beforehand. It can be e-mailed to: securityidunit@glasgowprestwick.com
- The participant organisation must phone the GPA Security ID Unit on 01292 511043 to make an appointment for the issue of the extension TEP(SRA)
- Both the employee and designated trained Escort must attend the Security ID Unit at the designated appointment time to collect the TEP(SRA)
- The employee must provide valid photo ID (Passport or Photo Driving Licence) and their Criminal Records Check i.e., UK Basic Disclosure Certificate. The Certificate will be checked for disqualifying convictions. If the Criminal Records Certificate has not yet been received, a 15-60 days TEP (SRA) cannot be issued until it is received – in the meantime, only a TEP (non SRA) can be considered
- The trained Escort will need to show their Airside (SRA) AIC, confirm they are an approved Escort (and have completed the GPA Escort Training) and fully understand their responsibilities.

Where a TEP(SRA) holder is judged by GPA to have an exceptional and legitimate reason for access to the SRA beyond 60-days, the holder may be permitted access for a further 14 consecutive calendar days. However, GPA will need to conduct a Risk Assessment and provide notification to the Civil Aviation Authority. This may apply if there are unforeseen circumstance like:

- The works is not yet completed due to unforeseen technical issues; or
- There is a genuine reason why a background check is not complete i.e., company offering a reference is no longer trading and a reference from another participant organisation (such as HMRC) is required; or
- There have been issues/breaches in escorting the TEP(SRA) holder e.g., they did not have the appropriate identity documents with them

The TEP(SRA) must always be returned to the GPA Security ID Unit at the end of the validity period.

5.6 Temporary Visitor or Employment Pass – SRA Access NOT Required

Any contractor(s) carrying out work to the fabric of an airside tenanted building **or** working on an airside apron/taxiway must obtain any Temporary Visitor Pass from the GPA Security ID Unit at the same time as any Work Permit (as per the GPA Contractor Control Policy).

For all others, when SRA access is not required, a Temporary Visitor or Employment Passes can be issued by GPA or any participant organisation **approved by** GPA. This currently consists of:

- GPA Security ID Unit
- GPA Central Search Security (when the ID Unit is closed)
- GPA Executive House (FBO)
- GPA Airfield Operations
- GPA Fire Station
- Prestwick Aircraft Maintenance Ltd (Ryanair) – as approved by GPA
- Chevron Aircraft Maintenance Ltd (Storm Aviation) – as approved by GPA
- Prestwick Flight Centre – as approved by GPA
- Prestwick Flying Club – as approved by GPA
- Bristows Search & Rescue – as approved by GPA
- HMS Gannet – as approved by GPA

NB: Any participant organisation who want to gain approval to issue non-SRA Temporary Visitor/Employment Passes should contact the Security ID Unit on 01292 511043 or securityidunit@glasgowprestwick.com

There is no limit to the duration of an airside (non-SRA) Temporary Visitor or Employment Pass, however, the temporary visitor/employee must be escorted all times whilst airside. The maximum Escort ratio is 1 to 10.

When the approved participant organisation is issuing either a Temporary Visitor or Employment Pass, the following guidance must be adhered to:

- The pass issuer must see valid photo ID (Passport **or** UK Photo Driving Licence) from the visitor/employee to confirm their identity. If the visitor/employee does not have valid photo ID, then **two** of the following must be provided:
  - Birth Certificate
  - A Biometric Residence Permit
  - A Settlement Permit (or Indefinite Leave to Remain)
  - A Residence Card
  - A Work/Study/Family Visa
  - A recent Utility/Council Tax Bill
  - A Bank Card or Bank Statement
  - A Debit or Credit Card
  - An Employer ID Card
  - A Further Education ID Card
  - A Young Scot Card
  - For a group of school age children for educational purposes – they are listed on a signed statement/letter from a Teacher/Group Leader that states they are registered at the school/group and how long the Teacher/Group Leader have personally known the child. This statement/letter must be on an original letter headed document, and give the full name, position, address and telephone number of the Teacher/Group Leader who has signed the document.
- The pass holder cannot carry out any work to the fabric of an airside tenanted building **or** be working on an airside apron/taxiway. When a contractor(s) is carrying out work to the fabric of an airside tenanted building **or** working on an airside apron/taxiway any Temporary Visitor Pass must be obtained from the GPA Security ID Unit.
- The pass holder must carry their valid ID at all times
- The pass must clearly show the full name of the visitor/employee and be clearly visible at all times (i.e., at chest height)
- The pass must clearly show the validity period
- The pass must be returned to the point of issue at the end of the validity period
- The participant organisation must keep a record of all temporary visitor/employment passes issued and make this available to GPA during any investigations, audits or inspections

GPA Security ID Unit Requirements:

- The participant organisation requesting the TVP(non-SRA) must send a completed Form IDPS 06 – TVP Application to the Security ID Unit at least 24 hours beforehand. It can be e-mailed to: securityidunit@glasgowprestwick.com
- The participant organisation must phone the GPA Security ID Unit on 01292 511043 to make an appointment for the issue of the TVP(non-SRA)
- Both the visitor and designated trained Escort must attend the Security ID Unit at the designated appointment time to collect the TVP(non-SRA)
- The visitor must provide valid photo ID (Passport or Photo Driving Licence) and carry it with them at all times
- The trained Escort will need to show their Airside (non-SRA) AIC, confirm they are an approved Escort (and have completed the GPA Escort Training) and fully understand their responsibilities

- The participant organisation must also ensure the necessary paperwork has been supplied as per the GPA Contractor Control Policy i.e., RAMS, PLI, Work Permit, etc.

5.7 Escort Responsibilities

Any participant organisation who issues (or, for the SRA, asks the GPA Security ID Unit to issue) an airside Temporary Visitor Pass (TVP) or Temporary Employment Pass (TEP) must always provide a suitable Escort.

Aviation Security Regulations states an Escort must:

- Be suitably trained; and
- Hold a valid AIC for the area in which escorting i.e., if escorting in the SRA, the escort must hold a valid AIC(SRA) for the appropriate areas; and
- Have the escorted person(s) in direct line of sight at ALL times; and
- Be reasonably sure that no security breach is committed by the person being escorted
- Not exceed the following escort ratios:

Escorting	**Maximum Ratio**
Temporary Visitor Pass Airside (not SRA)	1 Escort to 10 Visitors
Temporary Visitor Pass Airside (includes SRA)	1 Escort to 6 Visitors
Temporary Employment Pass Airside (not SRA)	1 Escort to 10 Employees
Temporary Employment Pass Airside (includes SRA)	1 Escort to 3 Employees

In addition, the Escort must:

- Be in attendance when the TVP or TEP is issued; and
- Present the escorted person(s) at all SRA Security Access Points, when appropriate; and
- Ensure the escorted person (s) always leaves the SRA through a Security Access point; and
- Not conduct any core responsibilities when escorting. The escort must maintain duty of care over the escorted person(s) at all times; and
- If a TEP holder is carrying tools of the trade (TTA), make sure these are authorised and properly controlled; and
- Ensure that the TVP or TEP holder has the appropriate identity documents with them, to validate the pass, at all times; and
- Ensure that the TVP or TEP holder has their name, contact details and is aware of what to do in an emergency; and
- Understand they are responsible for the safety and security of the TVP or TEP holders at all times whilst airside. This may mean waiting at the toilet entrance when a toilet break is required by the TVP or TEP holders; and
- Understand, if a TVP or TEP holder cannot be escorted by the same person for the duration of the visit, they are responsible for ensuring that the new escort is aware of their responsibilities and has signed as having taken over the escort duties; and
- Report to GPA Security any suspicious behaviour of the TVP or TEP holder(s) i.e., asking probing questions about the airport and security regimes, wanting to photograph areas that are not relevant to their visit or requesting to go to other areas that have not been authorised; and
- Remember that the TVP and TEP holder is under their supervision until they physically leave the confines of the airside area; and
- Ensure, when the visit or temporary employment is complete, they remove the TVP or TEP and return it to the issue point to be logged in and securely destroyed; and
- Understand they may be escorting a member of the Emergency Services in an Emergency Situation; in which case neither a TVP nor TEP is required.

Violations by a TVP or TEP Holder

If any person(s) becomes engaged in activities other than those for which they have been contracted or supports the purpose of their visit, escorted access must cease immediately, and the person(s) escorted

from the Airport. If the person(s) refuse to leave when requested, they are committing an offence under the Aviation Security Regulations. The Escort should immediately contact Security and the Airport Police

5.8 Summary of GPA TVP and TEP Vetting & Escort Requirements

The table below summarises the issue and escort requirements for airside TVP and TEPs:

Airside Temp Pass	Issue Requirements	Escort Requirements	Max Duration
TVP (SRA) Must be issued by GPA Security ID Unit	• Identity Check – Valid Photo ID (Passport or Driving Licence)	• Must hold a current Airside (SRA) AIC • Must have completed the GPA Escort Training (or GSAT since Jan 2021) • Escort max 6	1-7 days (no more than 14 days in a 12 month rolling period) Must be a 3 day break between issue
TEP (SRA) 1-14 days Must be issued by GPA ID Unit	• Identity Check – Valid Photo ID (Passport or Driving Licence) • Proof of application for Criminal Records Check	• Must hold a current Airside (SRA) AIC • Must have completed the GPA Escort Training (or GSAT since Jan 2021) • Escort max 3	1-14 days
TEP (SRA) 15-60 days Must be issued by GPA ID Unit	• Identity Check – Valid Photo ID (Passport or Driving Licence) • Copy of Criminal Records Check Certificate	• Must hold a current Airside (SRA) AIC • Must have completed the GPA Escort Training (or GSAT since Jan 2021) • Escort max 3	15-60 days
TVP or TEP (non SRA) Issued by GPA or an **approved** Participant Organisation	• Identity Check – Valid Photo ID (Passport or Driving Licence)	• Must hold a current Airside AIC • Must have completed the GPA Escort Training (or GSAT since Jan 2021) • Escort max 10	No maximum
TEP (non SRA) for Contractors doing works Must be issued by GPA Security ID Unit	• Identity Check – Valid Photo ID (Passport or Driving Licence)	• Must hold a current Airside AIC • Must have completed the GPA Escort Training (or GSAT since Jan 2021) Escort max 10	No maximum

6 THE FACE-TO-FACE SECURITY INTERVIEW

It is important that there is an initial assessment made as to the applicant's eligibility and suitability to hold any airside AIC that allows unescorted access. The AS must conduct a face-to-face Security interview as it is the perfect opportunity to question and obtain any necessary supporting information that may be required to substantiate the information already provided by the applicant. Information supplied by an applicant must not be accepted at face value by the AS.

The face-to-face Security Interview should normally be conducted by the AS; however, it can be conducted by another person who has been suitably trained by the AS – a declaration of this training must be held for investigation, audit and inspection purposes.

Participant organisations may incorporate the requirement for a Security interview as part of their recruitment and pre-employment screening procedures. However, it is also acceptable for the Security interview to be held once selection for employment has been made and a decision to apply for an Airside AIC has been taken. However, GPA accepts no responsibility if subsequently, it is determined the applicant cannot be issued with an GPA AIC i.e., they have an unspent disqualifying conviction.

6.1 The Purpose of the Face-to-Face Security Interview

The purpose of the Security Interview is to ensure that:

- the applicant can provide valid Proof of Identify that can be checked; and
- all periods over the preceding five years can be accounted for so that references and other supporting information can be obtained by the AS when conducting the Standard Background Check; and
- the applicant is able to meet the requirements for a Criminal Record Check and has no convictions that would disqualify them from holding an Airside AIC; and
- the applicant is fully aware of the checks that will be done to verify the information provided and provides all necessary consents; and
- there are no indications that the applicant may not be a suitable person to be given unescorted access to the Airside Area of the Airport

The Security Interview plays an integral part of the background check process because:

- it encourages the applicant to be honest (you could look at the applicant's digital social media footprint); and
- it allows the interviewer to find out missing information which is relevant to the pass application process and to probe applicants about their responses, or for additional information; and
- It provides a good opportunity to add to the overall assessment of the applicant's reliability and integrity

6.2 Conducting the Face-to-Face Security Interview

When conducting the face-to-face Security Interview with the applicant:

- the interviewer should prepare for the face-to-face Security Interview by reviewing all information already held for the applicant i.e., completed application form, etc.
- Form IDPS 03 - New Starter Security Interview Form and IDPS 03A – New Starter Security Interview Form Completion Notes should be utilised and will guide the interviewer in a systematic manner
- the applicant should be advised at the start of the interview that knowingly or recklessly making a false statement in connection with an application for an Airside AIC is a criminal offence under the

Aviation Security Act 1982, as amended by the Aviation and Maritime Security Act 1990 and will lead to automatic refusal of the application

- the interviewer should obtain consent from the applicant for the employer and/or GPA to contact previous employers and other potential referees
- the applicant should be advised that, where considered appropriate, further enquiries may be made to establish or verify facts. This may include checks on their online presence, previous AIC pass holding history, reasons for leaving employment and may involve passing information to the Police or other Security Agencies

There is a risk that an applicant may lie to the interviewer, present misleading information, or try and cover up something material that would otherwise prevent them from being suitable to hold an Airside AIC.

Whilst this may be considered unlikely, an applicant may even pretend to be someone else or present forged or counterfeit documents. The steps below are designed to give the AS, or another suitable trained person, the best chance of detecting deception.

However, any inconsistencies should be explored with the applicant sensitively, as there may be genuine reasons why an applicant is not being completely open on all relevant facts.

6.3 Conducting a New Starter Security Interview Virtually

In exceptional circumstances, when a face-to-face interview is just not possible, a New Starter Security Interview may be conducted via video conferencing facilities such as Zoom, MS Teams, Skype, Facetime, etc. The guidance on remote interviewing found on the Centre for the Protection of National Infrastructure (CPNI) Website must be followed: Click Here

Additionally, a physical check of all ID documents verified through this route will need to be completed at the earliest suitable opportunity (e.g., when the person reports for work).The AS should also establish a process to allow confirmation that the person interviewed virtually is the same person who starts work (e.g., a screenshot of the person during the interview).

6.4 The New Starter Security Interview Form and Completion Notes

Form IDPS 03 - New Starter Security Interview Form and IDPS 03A – New Starter Security Interview Form Completion Notes have been supplied with this Guidance and it is strongly recommended this form is used during the face-to-face Security Interview to ensure the necessary information is collected to effectively complete the Standard Background Check.

6.5 Section A: Applicant Personal Information

In this part of the form the interviewer will record the following information provided by the applicant, some of which may be pre-completed from their application form, etc:

- Full name (and any other known as, or previous names)
- Gender and Date of Birth
- Place of Birth and Nationality
- Contact details and National Insurance Number
- Address (and any previous addresses in previous 5 years)
- Any continuous periods of residence abroad for 6 months or more in previous 5 years

6.6 Section B: Identity Check

Of all the elements of the face-to-face Security Interview, the identity verification is the most fundamental. It should be the first check that is performed, and the interviewer must feel assured that an applicant's identity can be proven satisfactory – this may involve further checks after the interview.

It is expected that the identity document(s) presented by the applicant are copied (please write on the copy 'Original Seen' and sign/date underneath), recorded in Section B and closely inspected by the interviewer to establish that it is genuine and valid; and that it corresponds to the applicant.

The Approved documents with photographic ID are:

- **For British Nationals:** a valid full Passport or British Photo-card driving licence
- **For EU/ EAA and Swiss Nationals:** a valid full passport of National Identity Card
- **For all other Nationalities:** a full passport PLUS original Home Office document confirming right to work in the United Kingdom (such as a visa/ entry clearance/ humanitarian protection status) or a biometric Residence Permit for foreign Nationals issued by the Home Office that holds biographical data and biometric information and shows their immigration status and entitlements while resident in the UK

The interviewer, as a minimum, should then:

- Compare the photograph on the official identity document(s) with the applicant (in order to prevent instances of imposters, or 'look-alikes')
- Check the applicant's details on the official identity document(s) matches the information already provided
- Ask the applicant to write their signature and check it against the official identity document(s)
- Closely examine, in the presence of the applicant, the official identity document(s) for alteration or signs the photograph has been tampered with or replaced
- Where possible, have a genuine version (UK passport and Photo-Card Driving Licence) to hand and compare the documents. Check the feel of the paper, look to see if the type face is the same, tilt the document to reveal any expected watermarks, embossed stamps, etc.

There is further guidance available to establish if an official identity document is genuine. Below are several sources of good information available on the internet:

- The UK Government Home Office Guidance on Examining Identity Documents provides examples of genuine and counterfeit documents and describes the basic check that can be done: Click Here
- The National Protective Security Authority (NPSA) Good Practice guide on employment screening provides detailed guidance on document verification: Click Here
- The EU Public Register of Authentic Identity and travel Documents Online (PRADO) shows examples and describes security features that may be examined for passports and identity documents from EU member states, Iceland, Norway and Switzerland: Click Here
- The UK Government offers guidance for employers: Click Here

If the Applicant does not have an Approved Document with Photographic ID

Where the interviewer is satisfied the applicant, whose identity is to be established, cannot reasonably provide the approved documentation required, the applicant must supply the following ORIGINAL documents:

- A birth of adoption certificate; or
- A registration or naturalisation document: and
- Proof of residence in the UK; and
- A passport sized photograph, endorsed on the back with a signature from a Justice of the Peace, Medical Practitioner, Officer of the Armed Forces, Clergyman, Teacher, Lawyer, Bank Manager or Civil Servant who has known the applicant, either personally or professionally, for a minimum of 3-years. The signed photograph must be accompanied by a signed statement from the photo signatory, in an original letter headed document, giving their full name, position, address and telephone number stating the period and capacity in which they know the applicant

A supplementary approach is to use electronic databases to verify identity. This involves an approach which does not solely rely on any physical assessment of paper documents. By searching for electronic records associated with the name, date of birth and addresses provided by an applicant, it is possible to

build a picture of the applicant's past and current life. A long history of varied transactions and events indicates that the identity is more likely to be genuine. A history that lacks credible detail and/ or depth may indicate that the identity is false.

Database checks alone are not sufficient to confirm that the applicant is the rightful owner of that identity- they simply confirm that the identity exists. In this case, the Security Interviewer must test the applicant's knowledge of the information that has been obtained from the electronic check to confirm that the applicant owns and is rightfully using the identity.

There are also a large number of suppliers that may be able to perform an identity check for the AS to the required standard – for a cost. These companies can be found by doing an internet search. However, it is important the AS does their own research of the company offering the service and they understand how the supplier arrive at their results and how they report their findings.

Verfy.gov.uk – there is also a government services that can be used by individuals free of charge to have their identity verified electronically. If they have a driving licence, the AS could ask the person to use verify.gov.uk to obtain a licence 'check code' valid for 21 days. Before a check code is provided, the person's identity is verified via DVLA and other databases. If the person the gives the check code and the last 8 digits of their driving licence to the AS, the AS can use these to confirm the validity of the licence. This is a much more robust system than relying on a visual check of the driving licence alone. More information is available here

Overall, the information collected by the interviewer must allow the AS to confirm:

- The identity presented by the applicant is genuine and relates to a real person
- The applicant owns and is rightfully using that identity.

6.7 Section C: Check of Previous AICs Held

It is important for the AS to establish if the applicant has previously held an Airport Identity Card for GPA or any other airport and if they have ever had a pass withdrawn to make sure an AIC is not issued to someone considered unsuitable who might pose a threat to aviation security.

The interviewer should ask the applicant to confirm the details of any previous AIC(s) held which should include which airport(s), the pass sponsor i.e., employer/participant organisation, the AIC number (if known) and the reason it was withdrawn. This information should be recorded at Section C by the interviewer.

6.8 Section D: Criminal Convictions Check

If the applicant has a criminal conviction(s) that disqualifies them from holding an AIC, this should be identified early in the process as this may negatively impact any job offer.

The interviewer should ask the applicant if they have any unspent criminal convictions. This includes convictions in all countries, not just the UK. This information should be recorded at Section D by the interviewer.

See Part 7.5 regarding Disqualifying Convictions.

6.9 Section E: Previous 5 Year History

The AS must be able to independently verify what the applicant has been doing during the preceding 5 years as part of the Standard Background Check to ensure:

- The employment, education or benefit history is genuine and relates to the applicant

- The applicant is not concealing something from their history that might pose a threat to aviation security

The interviewer should obtain this information from the applicant and record it in Section E. The following should be noted:

- The 5-year history should be done in chronological order, with the most recent first
- If the applicant has been employed, they should note the start/end date, employers name and address, position held, reason for leaving and the contact details of a person or department within this company/participant organisation who will be able to confirm this period of employment.
- If the applicant has been in education, they should note the start/end date, educational establishment name and address, course studied, reason for leaving and the contact details of a person or department within this educational establishment who will be able to confirm this period of study.
- If the applicant has been in receipt of Benefit, they should note the start/end date, the paying Government Department's name and address, the Benefit claimed and the contact details of a person or department within this Government who will be able to confirm this period on Benefit.

All **gaps over 28-days** between periods of employment, education or being in receipt of benefit **must be accounted for**. If there are gaps in excess of 28-days, the interviewer should ask the applicant for the name. address and contact details of a person(s) who will be able (and willing) to confirm, from their own personal knowledge of the applicant, what the applicant was doing during these gaps. This is known as providing a Gap or Personal reference. The person(s) cannot be a member of their family or in a close personal relationship with the applicant, but they must have personally known the applicant during the full period of the gap in question.

Gap/Personal references may be used by an applicant to mask actual activity undertaken such as employment so, in addition to the Gap/Personal reference, the interviewer should explore with the applicant what other supporting evidence might be available. This is particularly important when there are extended gaps such as periods of extensive travel or maternity. For example:

Periods of extensive travel could be supported by:

- proof of itinerary, travel documentation,
- a passport containing visa stamps for the countries visited
- suitable proof of residence for the time spent abroad i.e., document from landlord, hotel bills, etc.
- bank/credit card statements showing spending overseas
- contact details of acquaintances met overseas including dates/places of meeting

Periods of maternity could be supported by:

- child's birth certificate
- confirmation of Child Benefit claim

Any supporting evidence that might be available will be dependent on what the applicant was doing during the gaps. The interviewer should ask the applicant what's available as supporting evidence and use common sense in deciding what is reasonable to request.

6.10 Section F: Additional Notes

The interviewer should use Section F to record any additional notes and/or overflow from any other Sections on the form.

6.11 Section G: Applicant Declaration

The interviewer should read the statement and then ask the applicant to sign the form at Section G confirming they understand the implications of making a false statement and giving their consent for the AS to contact former employers, educational establishments, Government Agencies and Gap/Personal references for verification of the information provided.

6.12 Section H: Applicant Suitability and Interviewer Declaration

The interviewer needs to confirm they have obtained all the necessary information and have assessed the credibility of that information to move to the next stage of the process. To assess whether the information provided by the applicant appears credible, the interviewer should make an overall assessment as to whether the Standard Background Check is likely to be straightforward or if there is something that will require investigation:

- Has the applicant declared a disqualifying criminal conviction?
- Has the applicant given inaccurate or inconsistent answers?
- Has the applicant provided an identity document that appears to have been tampered with or may be counterfeit?
- Was the applicant unable to account for all of the preceding 5 years?
- Has the applicant got significant gaps between period of employment/education/in receipt of benefit and unable to provide a person(s) to provide a Gap/Personal reference and/or supporting evidence?
- Has the applicant been residing overseas during the preceding 5 years?
- Has the applicant done any unusual travelling such as visiting countries that have not been recommended by the Foreign & Commonwealth Office?

The above list is not exhaustive.

The interviewer should keep their notes factual and be careful not to express an opinion. Any notes made may be disclosed to the applicant at a later date.

The interviewer should read the statement and then sign and date Section H.

6.13 The Applicant Request a Copy of the New Starter Security Interview Form

If an applicant requests a copy of the New Starter Security Interview Form, a full copy of the form must NOT be provided, as it could leave the process vulnerable to abuse. A suitably redacted version can be provided.

7 THE STANDARD BACKGROUND CHECK

It is the Authorised Signatory (AS) who must conduct the necessary background checks on any Airside AIC applicant before approving and submitted the application form to the GPA Security ID Unit.

Background checks on an applicant have an important security value and cannot be approached in a mechanistic manner. An element of judgment will often be required. Conducting checks will often be a time consuming and complex process.

It is therefore important that an assessment is made at an early stage that an applicant is likely to be able to meet the criteria for an Airside AIC i.e., during recruitment. For example, if a successful job applicant is going to need an Airside AIC, it is important to consider the following five questions during the recruitment process:

- Will the applicant be able to provide the required Proof of Identity?
- Does the applicant have an unspent criminal conviction that is a Disqualifying Offence?
- Is the applicant able to provide full details of what they have been doing over the last five years?
- Can you establish the applicant's airport pass-holding history?
- Are you sure that the applicant has a genuine operational need for airside access?

The AS should ensure that all anomalies have been adequately addressed prior to submitting the application. In complex cases decisions on suitability should involve the business areas that have a vested interest. Consideration should be given to the role that the applicant will be undertaking and their integrity.

It simply might not be possible for the Authorised Signatory to put forward an AIC application to GPA, as sufficient assurances might not be achieved regarding gaps in information. This should not reflect adversely on the applicant or cast any doubt on their character.

7.1 Standard Background Check Requirement

Under UK Aviation Security Regulations, the application process for an Airside AIC must include a Standard Background Check. As a minimum, this check must include:

- obtaining valid Proof of Identity
- obtaining a Criminal Records Check (CRC) Certificate to ensure the applicant does not have any disqualifying convictions.
- conducting a 5-year employment, education and periods in receipt of benefit check
- obtaining a Gap/Personal Reference for any periods, over 28 days, in the preceding 5 years the applicant has not been in employment, education or in receipt of benefit
- obtaining details of any other Airport Identify Cards/Passes currently or previously held
- where appropriate, obtaining Proof of Right to Work in the United Kingdom

7.2 Obtaining Valid Proof of Identity

Valid proof of identity should already have been obtained during the face-to-face New Starter Security Interview - see Part 6.6. The AS should make sure they write on the copy of the ID 'Original Seen' and sign/date underneath.

NB: Once the AS has obtained valid proof of identity (and the application is going to be for an AIC **with SRA Access**) it is good practice for the AS to send the GPA ID Security Unit Form IDPS 12 - AIC SRA Accreditation Check Request before the other elements of the Background Check have been completed. GPA must request an Accreditation Check via UK National Security Vetting (UKNSV) for all AIC applicants who need SRA access. Once the request is made by GPA, UKNSV will take a minimum of 5 calendar days to respond. Sending the form to request the Accreditation Check before submission of the full AIC(SRA) Application will speed up the time needed from application submission to issue of the AIC(SRA). See Part 8 of this Guidance for more information on the Accreditation Check.

7.3 Obtaining a Criminal Record Check Certificate

It is important that the Authorised Signatory (AS) verifies that the applicant has not been convicted of any criminal offence that would disqualify them from holding an AIC.

The AS must obtain a valid Criminal Record Certificate (CRC) from the applicant for all the countries the applicant has resided, for 6-months or more, during the previously 5-years. This applies even if the applicant already holds a UK National Security Vetting Clearance (CTC, SC, DV).

Any CRC must be dated within 10 weeks of the AIC issue date so, where an overseas CRC is needed, the AS will need to factor any additional time into the process.

How to obtain a UK Criminal Record Certificate (CRC)

A Basic Disclosure is required showing any unspent convictions under the Rehabilitation of Offenders Act 1974. The procedures for obtaining a UK Basic Disclosure CRC are straightforward:

- Applicants living and working in Scotland should apply for a CRC from Disclosure Scotland: Click Here
- Applicants living and working in England and Wales can obtain a CRC from the Disclosure and Barring Services ((DBS): Click Here
- Applicants living and working in Northern Ireland can obtain a CRC from Access Northern Ireland: Click Here

All of the above CRCs will return any **UK wide** unspent convictions.

An applicant can apply for a CRC online, however, the UK agencies do offer a service that allows employers to register and submit requests for Basic Disclosures on behalf of an employee. In all cases, the original CRC will be posted to the applicant. The applicant should then present the original document to the AS for checking.

Please also note, any criminal activity for all UK service personnel, whether serving at home or abroad, will be recorded on their UK criminal record and will show up on a basic disclosure. As such, as long as the person was a serving member of the armed forces during any periods of overseas deployment, the criminal record check element of a background check or enhanced background check can be satisfied with a UK CRC where this is less than 10 weeks old. There is no need to get a separate overseas CRC for that period.

How to obtain an Overseas Criminal Record Certificate

Where an applicant has been continuously resident in an overseas country for 6 months or more during the previous 5-years, an Overseas CRC must be obtained. The application process for an Overseas CRC varies and is not always straight forward.

Country specific advice including local application procedures is available at both, the National Protective Security Authority (NPSA): Click Here and Gov.UK: Click Here

Cannot Obtain an Overseas CRC

Exceptionally, it may be the case, the Authorised Signatory (AS) simply cannot obtain an Overseas CRC having made a reasonable effort to do so. Where an AS is able to demonstrate to GPA's satisfaction that there are exceptional circumstances as to why an Overseas CRC cannot be obtained, GPA may accept a sworn oath by the applicant witnessed by a Commissioner for Oaths, as an alternative.

A Commissioner for Oaths is a person who is authorised to verify affidavits, statutory declarations and other legal documents. Affidavits are statements in writing and on oath, and statutory declarations are written statements of facts that the person signs and declares to be true.

For persons who have served overseas in the military, an extract from their military record will also be accepted. The extract must:

- Be a colour copy taken from the original document, not a copy of a copy
- Cover (and state that it covers) all of the periods within the past 5 years during which the person was overseas for 6 continuous months or more and serving in the military. (e.g., overseas tour or Operational deployment).
- Expressly disclose any and all convictions that may have been received during this time
- Be from an identified source that can be contacted if there is a need to verify the extracts authenticity

GPA will only accept these alternatives in cases where:

- A government administration has collapsed to a point where no credible official sources of information exist
- There is a credible risk to the individual personal safety if they make contact with that country e.g., where an individual has applied for asylum status in the United Kingdom
- Any requests for such information need to be individually supported by the UK Government
- A request is declined due to local policies - often the case where residency is disputed by the appropriate authority e.g., tour operator employees

7.4 Checking that the Criminal Record Certificate (CRC) is genuine

When received, the applicant should present the original CRC to the Authorised Signatory (AS) for checking and copying. After checking and verifying, the AS should photocopy (colour if possible) the CRC and return the original to the applicant. The AS should write on the copy 'Original Seen' and sign/date underneath.

Security Features of a UK CRC

A UK CRC contains a number of security features which can be used to verify whether it has been counterfeited or altered in any way:

- A 'Crown Seal' watermark repeated down the right-hand side of the certificate, which is visible both on the surface and when holding the certificate up to a light source
- A background design with the word 'Disclosure', which appears in a wave-like pattern across both sides of the document- the colour of this pattern is uniform across the front of the certificate between pink and green on the reverse side
- Ink and paper that will change colour in the presence of water or solvent based liquid

How to Verify that an Overseas CRC is Genuine

In the absence of a verified original copy, it may be difficult to establish with all certainty that an overseas CRC is genuine, however there are some steps the AS can take:

- Where possible, apply direct for the certificate from an official government, embassy or consular sources- consent from the applicant will be required
- Authenticate a certificate obtained by an applicant by contacting the issuing authority to verify the certificate serial/reference number
- Obtain a reliable translation where the certificate is not written in English- free web-based translations are NOT satisfactory
- Compare the certificate with examples provided in the guidance from CPNI or Gov.UK

The AS must always closely examine the original CRC or Overseas CRC to:

- confirm that the date of issue is going to be within 10 weeks of the AIC issue date
- confirm that the CRC corresponds to the applicant - the first and last name and date of birth on the CRC must match exactly the name on the applicant's official identity document
- take all reasonable steps to examine the CRC for any signs of tampering or counterfeit

If the AS is doubtful whether a certificate is genuine, or if they think that it may have been altered, they should contact the issuing authority.

7.5 Checking for Disqualifying Criminal Convictions

The CRC or Overseas CRC will either state that there are no convictions at the time of the application or will list details of convictions.

Where the CRC or Overseas CRC details a conviction for a disqualifying (or similar offence), an application for a GPA AIC will normally be refused, however, see the next section regarding a Certificate of Disregard.

The list of the most common disqualifying offences can be found on the CAA website: Click Here

Overseas convictions

It can be a challenge to interpret the information that is presented on an Overseas CRC. Convictions that are listed may not easily correlate to the UK list of disqualifying convictions and some listed convictions may be considered 'spent' under UK legislation.

The Authorised Signatory(AS) may need to make their own judgement as to whether the information presented may suggest that a person might pose a risk. In doubtful or complex cases, the AS may seek the advice from the GPA Security ID Unit before submitting an application.

7.6 A Certificate of Disregard

If a check of criminal records has revealed any unspent disqualifying conviction(s), the applicant will not normally be issued with an AIC. This is because unspent convictions for offences that involve violence, dishonesty or abuse of trust can indicate vulnerability to pressure or improper influence, or liability to committing a breach of security.

If the AS feels there are exceptional circumstances, the applicant may apply to the Secretary of State for Transport for a 'Certificate of Disregard'. Full instructions can be found at: Click Here

Applicants should note that if a certificate of disregard is granted, this does not mandate the issue of an AIC. The final decision on whether to issue an AIC remains at the sole discretion of the GPA Security Operations Manager.

7.7 Verifying the Applicant's 5-Year History

It is important that the Authorised Signatory (AS) independently verifies the 5-year history declared by the applicant is genuine to be confident the applicant is not concealing something from their history that might pose a threat to aviation security.

The method and quality of checks undertaken by the AS is paramount in preventing fraud or insider threat, so it is crucial the AS follows the approach set out in this Guidance and:

- independently verifies the information provided by the applicant at the face-to-face New Starter Security Interview and obtains written references from employers, educational establishments and government department to confirm any period in receipt of benefit
- independently obtains Gap/Personal references, where appropriate, to verify periods over 28 days when the applicant was not in work, education or in receipt of benefit
- checks the validity and reasonableness of any additional supporting evidence for periods over 28 days when the applicant was not in work, education or in receipt of benefit

It is recommended that a record for each applicant is maintained by the AS to show progress against each step in the 5-year history check process. In addition, all the records showing how the 5-year history was independently verified by the AS will need to be made available to GPA during quality assurance audits.

7.8 Important General Referencing Procedures

The AS must independently obtain or verify written evidence to confirm what the applicant has been doing and where they have been resident over the preceding 5-years (accounting for all periods of over 28 days between periods of employment, education or in receipt of benefit).

If the applicant has turned 16 years of age in the last 5 years, references are not required prior to the reference which includes the applicant's 16th birthday.

Firstly, the AS must satisfy themselves that the referee genuinely exists and/or works for the relevant participant organisation and that the contact information (address, telephone number and e-mail) is correct – this can be done using public sources and internet web searches. The AS must always independently check the validity of the contact information provided by the applicant.

Secondly, when contacting a referee in writing, it is recommended the AS uses a structured set of prepared questions for the referee to respond to. It's likely, most participant organisations already have this as part of their existing recruitment processes. Unlike a reference that might be obtained for employment purposes, where having an insight into the persons qualifications, skills, personal attributes and qualities is useful to determine their suitability for a job, a Standard Background Check reference simply needs to state some basic facts. Any reference template or letter, as a minimum, must adhere to the following standards to satisfy the requirements of the Standard Background Check:

- The referee must be made aware that it is the participant organisation that is requesting the reference so the participant organisation name must be visible either on the reference or the reference request or in the e-mail trail.
- The referee must be made aware their refence will be used for security purposes and that knowingly giving false information is a criminal offence, and could lead to prosecution, under the Aviation Security Act 1982, as amended by the Aviation and Maritime Security Act 1990.
- Where appropriate, be provided on the relevant company/participant organisation headed paper or stamped with the company/participant organisation stamp or be accompanied by a signed and dated company/participant organisation compliments slip.
- Contain the first and last names of the applicant as it appears on their identity document – shortened or known by names are not acceptable.
- Contain the full name, address, contact number and job title (if an employer) of the author
- Clearly state the specific dates covered by the reference i.e., start date and finish date
- Contain the date of issue
- E-mail references from a Company/Participant organisation must originate from their official domain e-mail address i.e., personnel@examplecompany.com
- The use of correcting fluid or a handwritten amendment/addition on references by the AS is NOT permitted. Any correction or amendment made must be countersigned by the reference author.
- The AS may keep 'file notes' in either handwritten or typed format to record the time and content of any meetings, telephone discussions or other events. For example, an explanation of the action taken to verify the identity of a referee, address an anomaly or to follow up a question and the respective outcome
- When references are not written in English, a translation by a certified translator is required. The contact details of the translator must be held so that credentials can be checked if selected by GPA for a Quality Assurance Check. Free web-based translation services i.e., google translator, are not acceptable.
- Confirms the whereabouts or activities of the individual during this time (appropriate for Gap/Personal references)

7.9 Referencing - Periods of Employment

1. A written reference or a 'certificate of employment' obtained by the AS directly from the employer is acceptable.

2. If contacting a referee by phone, after the phone call the AS must send an e-mail to the referee summarising the details and requesting a reply confirming it accurately reflects the information they provided. A print of the e-mail is acceptable.
3. If an applicant provides a written reference or 'certificate of employment' to the AS, it should **not** be accepted on face value. The AS is required to verify the referee exists and that they issued it. A record should be kept of this contact.
4. Where an employer fails to respond to a reference request, after a reasonable period of time, an employment history can be obtained from HM Revenue and Customs (HMRC). This can be requested by the applicant, or they can consent to the AS obtaining this. More information is available at: Click Here
5. If the AS obtains an HMRC reference and it does not provide actual dates of employment, a Gap/Personal reference must additionally be obtained.
6. Where the previous employer has ceased trading, the AS should obtain an HMRC reference (as per 4 & 5 above) and documentary evidence to support the fact that the company/participant organisation has ceased trading.
7. For agency employment, the AS should obtain a written reference from the Agency. The Agency should be asked to declare any periods of time between placements exceeding 28 days.

7.10 Referencing - Periods of Self-Employment

1. The AS should obtain a written reference from the applicant's solicitor or accountant.
2. Where there is no solicitor or accountant or they fail to respond to a reference request, after a reasonable period of time, an employment history can be obtained from HM Revenue and Customs (HMRC). This can be requested by the applicant, or they can consent to the AS obtaining this. More information is available at: Click Here
3. If the AS obtains an HMRC reference and it does not provide actual dates of employment, a Gap/Personal reference must additionally be obtained alongside additional evidence of self-employment during the relevant period. Poor self-employment records can make it challenging to adequately meet the referencing standard required. However, the onus is on the applicant to provide the AS with additional sufficient evidence to verify any periods of self-employment. This could include, but is not limited to:
    - business bank account statements showing deposits/withdrawals
    - rent/lease agreement for business premises
    - HP/lease agreement for any business vehicles
    - business insurance documents

7.11 Referencing – Periods in Education

1. The AS should obtain a written reference from the educational establishment.
2. If the educational establishment no longer exists, a Gap/Personal reference must be obtained alongside additional evidence of being in education. This could include, but is not limited to:
    - Certificates of qualifications obtained
    - letters from the educational establishment i.e., course offer letter.

7.12 Referencing – Periods in Receipt of Benefit

1. The AS should obtain a written reference from the relevant government department that paid the benefit. In the UK, this is normally the Department of Work & Pensions (DWP), however, some benefits may now be paid by devolved administrations i.e., Scottish Government. If the AS cannot obtain this

reference direct from the relevant government department, the applicant may request the reference and provide to the AS. On receipt, the AS needs to satisfy themselves the reference is genuine.

7.13 Referencing – Gap/Personal References

It can be particularly challenging for the AS to verify what a person has been doing and where they have been residing if they have not been working, in education or in receipt of benefit, particularly for extended periods.

With respect to education (within the same establishment) regular academic summer holidays of more than 28 days should generically be disregarded and so not need to be covered by a Gap/Personal reference. However, other periods of extended leave over 28 days such as sabbaticals and gap years do need to be covered by a Gap/Personal refence.

During the face-to-face Security Interview, the AS should already have identified any periods over 28-days (in the preceding 5-years), where the applicant was not in work, education or in receipt of benefit. The applicant should have provided the contact details of someone who has a personal knowledge of them during this period(s) and is willing to provide a Gap/Personal Reference. In addition, other supporting evidence should have been supplied or identified.

Firstly, the AS must be satisfied the individual providing the Gap/Personal Reference had regular and genuine contact (at least once every 28 days) with the individual during the period that the reference covers and have either:

- known the individual in a professional capacity
- known the individual in a personal capacity for a minimum of two years

Secondly, the individual providing the Gap/Personal reference must **NOT** be:

- a family member of or in close personal relationship with the applicant such as a blood relative, current or ex-relative by marriage, relatives by adoption- including cousins, current or ex-partners and their relatives
- someone who has a financial interest in the individual, such as a person who has provided financial support, or has a vested interest - such as a landlord
- under the age of 16

Once the AS is satisfied the individual is suitable to provide a Gap/Personal reference:

1. Obtain a written Gap/Personal reference from the individual.
2. It is good practice for the AS to speak directly to the Gap/Personal referee to confirm they had regular and genuine contact with the applicant and ask detailed questions about the period in question. However, after the phone call the AS must send an e-mail to the referee summarising the details and requesting a reply confirming it accurately reflects the information they provided. A print of the e-mail is acceptable.

Other Supporting Evidence

The Gap/Personal reference must not solely be relied upon as the referee may not have been in close contact with the applicant over the entire period or may lie to help the applicant cover up part of their history. This is particularly important if the Gap/Personal referee is vouching for an extended period of time or for several periods over the preceding 5-years. The AS should therefore **always** obtain other supporting evidence that corroborates the statements made by the applicant.

Supporting evidence can be anything that should be 'reasonably' available depending on what the applicant has been doing. It can include, but is not limited to:

- obtaining evidence of extended travel (tickets, passport visa stamps and hotel bills)
- confirming periods of maternity leave through a child's birth certificate or Child Benefit claim
- obtaining bank statement showing transactions during the relevant period
- obtaining a letter from an individual who was supporting the applicant financially
- checking public social media accounts for the applicant and the referee

7.14 Checking an Applicants Airport Identity Card (AIC) Holder History

It is very important that an AIC is not issued to someone already considered unsuitable who might pose a threat to aviation security. During the face-to-face Security Interview, the applicant should have already provided details of any previously held AICs as follows:

- Issuing Airport
- Sponsor (employer/participant organisation)
- AIC Number (if known)
- Reason for withdrawal/cancellation

The AS is also required to:

- Check the applicant's employment history to identify and resolve any inconsistencies. For example, have they declared previous working at an airport but have stated they have never held an AIC?
- Complete the details of previous AICs held by the applicant on the relevant AIC Application Form – the GPA Security ID Unit will conduct the necessary checks with the previous issuing Airport.

If the AS has any concerns or doubts, they should contact the GPA Security ID Unit.

7.15 Proof of Right to Work in the United Kingdom

When an AS is applying for an AIC for an **employee** of their company/participant organisation, their Human Resources (HR) Department should have already obtained evidence of their right to work in the UK before any offer of employment. This is a legal requirement and consists of either a Share Code provided by the applicant (issued by the Home Office) or a check of original documents.

The check of original documents is normally the same/similar to the Identity Check required as part of the Standard Background Check, however, they should not be confused. They are not the same and whilst the same original documents may be used, they should be recorded separately.

However, the applicant's right to work may affect the normal validity period of the AIC issued. The AS must contact their HR Department to confirm:

- the applicant has the right to work in the UK
- any restrictions on the duration of their right to work in the UK

The AS will need to complete the right to work details on the relevant AIC Application Form.

8 THE ENHANCED BACKGROUND CHECK & ACCREDITATION CHECK

From 1st January 2022, under UK Aviation Security Regulations, any AIC/CIC applicant who needs access to the Security Restricted Area (SRA), must undergo an Enhanced Background Check. The Enhanced Background Check consists of the Standard Background Check plus an additional Accreditation Check (AC) and can last up to 5-years.

8.1 The Accreditation Check (AC)

The AC is a new level of UK Security Vetting (UKSV) that will have a lifespan of up to 5-years and will be conducted on all new/renewal applicants for AIC/CICs, that include access permissions to the SRA, from 1st January 2022.

The Enhanced Background Check and AC lifespan of 5-years will only be appropriate if the AIC holder's information is provided to the Access Pass Holder Information Distribution System (APHIDS) – see Part 9 of this Guidance. A mandatory 12-month review of the AC can then be conducted via APHIDS which means a new AC only needs to be requested every 5-years. If not, the Enhanced Background Check and AC will only have a lifespan of up to 12-months.

An AC is still required even if the AIC/CIC (SRA) applicant already holds another level of Security Vetting Clearance i.e., Counter Terrorism Check (CTC), Security Check (SC) and Developed Vetting (DV).

8.2 Applying for the Accreditation Check (AC)

Only UK Airport Operators or Air Carriers can apply to UKSV for the AC. The AC request will be sent to UKSV by GPA when the AIC (SRA) application is received. Once the request is made, UKSV will take a minimum of 5 calendar days to respond and will only

However, the AC can be requested as soon the applicants ID is verified by the AS – the full background check does not need to be complete. This means the AS can complete and e-mail Form IDPS 12 - AIC SRA Accreditation Check Request to the GPA Security ID Unit on securityidunit@glasgowprestwick.com before the full application is submitted. This will speed up the time needed from application submission to issue of the AIC(SRA).

Please note the CAA will charge GPA for all AC requests made. This cost is recovered by GPA within the charge for an AIC (SRA) when it is issued. However, if an AC is requested and an AIC (SRA) is not subsequently issued (for any reason), the AC cost, plus an additional admin amount detailed in Appendix 2 of this Guidance, will be charged to the Participant Organisation.

8.3 Accreditation Check Decision – Granted or Refused

The CAA will not pass on any details beyond the AC clearance decision and GPA will only be informed that a clearance is granted or refused.

Where an AC is refused, the AIC (SRA) applicant will also be notified along with details of their right(s) of appeal. In addition, any refusal will be communicated to the Participant Organisations Nominated Officer (NO) by the CAA. If an AC is refused, any AIC (SRA) cannot be issued and any existing passes must be withdrawn.

Existing employees who are not granted an AC will have a right of appeal to the CAA. Full details will be provided to the AIC (SRA) applicant as part of the refusal letter issued by the CAA. They will have 21 days to lodge their appeal and the CAA will aim to complete it within 28 days of receipt. If the CAA appeal upholds the original decision, existing employees may have a right to appeal to the Security Vetting Appeals Panel

(SVAP). In line with HMG National Security Vetting Policy, these appeal rights do not apply to applicants who were not already an existing employee.

8.4 AIC's (SRA) Issued Prior to 1st January 2022 – No Action is Required

The UK Security Regulations allows for all existing AIC (SRA) holders to undergo the Enhanced Background Check/Accreditation Check by 1st July 2024. For the majority of existing AIC (SRA) holders, this will be done when their current AIC (SRA) is due for renewal prior to 1st July 2024. Any others will be contacted directed by GPA between April-May 2024.

9 ACCESS PASS HOLDER INFORMATION DISTRIBUTION SYSTEM (APHIDS)

APHIDS is a joint Home Office (HO) and Department for Transport (DfT) developed secure system to enable the collection of data relating to all airside Airport Identity Card (AIC) holders and Crew Identity Card (CIC) holders. It will also be used to complete the regulated 12-month review of all those who have an Accreditation Check (AC) so they will only require a new Enhanced Background Check/AC every 5-years.

APHIDS captures all airside AIC/CIC date from all UK airports, including the personal address, phone number and email address of the ID card holder. This is used for both law enforcement purposes and, where appropriate, to keep the Accreditation Check (AC) and/or the AIC/CIC holders criminal records under review for the duration of the validity period of the AIC/CIC.

APHIDS will provide Law Enforcement Agencies the ability to identify potential insider threats at airports to help improve border and aviation security. Law Enforcement Agencies will be able to query across the APHIDS database to determine whether a subject of interest holds airside access to enable them to evaluate the potential threat they pose and support operational development of new leads.

9.1 Providing the Information to APHIDS

From 1st January 2022, GPA has a regulatory requirement to securely upload the information it holds on all airside AIC holders to APHIDS. The information uploaded will be taken from what's recorded on the GPA Access Control System (SiPass Integrated System) and AIC new/renewal application form.

The requirement to provide this information is wholly the responsibility of GPA and will be done by the GPA Security ID Unit on a weekly basis.

The new AIC application/renewal forms must be used by all organisations from 1st January 2022 to ensure the mandatory APHIDS information is being provided when a new/renewal AIC application is made.

10 A LEGITIMATE OPERATIONAL NEED TO ACCESS AIRSIDE

In addition to the current Standard Background Check and Enhanced Background Check (from 1st January 2022), the UK Aviation Security Regulations require that any applicant must have a legitimate operational need to access Airside areas to carry out their employment duties/activities.

The AS must satisfy themselves that the applicant has a genuine and legitimate operational need for airside access. They will need to determine the proper extent of the access required and provide a written justification for the access levels on the relevant AIC Application Form.

As a result, the AS will need to have a good understanding of the job role/activities that need to be undertaken by the applicant. This may require consultation with the line manager or another appropriate person within the company/participant organisation. The following aspects should be considered:

- Where is the applicant's normal place of work?
- Is access required on a regular or occasional (but necessary) basis and for what reason?
- If access is required to the Security Restricted Area (SRA), does the applicant need internal or external access (or both)?
- Are there any other areas needed?
- Is the access required to fulfil the requirements of a contract and access is limited to the duration of this contract?
- Is the access required for an existing statutory, government or public function?
- Is access required to perform essential airport or aircraft services – essential is defined as something vitally important to the safe and secure operation of the airport or an aircraft, including crisis management and business recovery activity?
- Have you already agreed 'core' access permissions for roles within your company/participant organisation with GPA?

Please note, the final decision rests with GPA. This may result in the issue of an AIC granting access to areas different from those originally requested by the AS. In such cases, a full explanation will be given to the AS.

11 MANDATORY TRAINING FOR ALL AIRSIDE AIC HOLDERS

It is important that all airside AIC Holders understand their responsibilities in contributing to a robust safety and security culture at GPA. Every AIC holder needs to ensure, at all times, they are adhering to the safety and security requirements that keep all employees, passengers, tenants and visitors at GPA safe.

Therefore, prior to the issue of ALL new or renewal AIC (Non-SRA) or AIC (SRA), the applicant will need to successfully complete:

- GPA Airside Safety Awareness Training (ASAT); and
- GPA General Security Awareness Training (GSAT)

Please note, new AIC applicants may only complete GSAT after the AS determines they have successfully completed their reference and criminal records checks.

11.1 Overview of Airside Safety Awareness Training (ASAT)

This E-Learning is specific to GPA and will be provided to the applicant at no cost. The applicant will need to successfully complete a knowledge Assessment after the training.

The objectives of the ASAT E-Learning training are:

- To ensure all airside personnel are aware of the rules and regulations governing Airside Safety
- To remain compliant with Glasgow Prestwick Airport Safety Management System policies
- To minimise the risk of accidents and injury to persons whilst airside
- To minimise the risk of damage to aircraft and property while working in an airside environment
- To ensure an understanding of the consequences for failing to comply with rules and regulations as governed by Glasgow Prestwick Airport.

The Assessment will be completed on-line via the GPA Redkite System and will consist of 20 random, multiple choice questions. To successfully pass the assessment the applicant must answer a minimum of 18 correctly (90%). The applicant will be allowed a maximum of 3 attempts to successfully complete the Assessment, after which time they will be locked out. If an applicant is locked out of the training, the AS (or their Line Manager) should contact the GPA Security ID Unit.

11.2 Overview of General Security Awareness Training (GSAT)

Please note regulation states this training can only be completed by the applicant after all elements of the Standard Background Check have been completed successfully by the AS.

This E-Learning, whilst not specific to GPA, does contain localised information and is provided by GPA at no additional cost. It is also available from other CAA approved providers (click here for a list of CAA approved providers). The applicant will need to successfully complete a knowledge Assessment after the training.

The objectives of the GSAT E-Learning training are:

- To ensure all airside personnel understand the threats to aviation
- Understanding of the current threat level
- Know who may pose a threat to aviation
- Know the possible motives of those people who may pose a threat to aviation
- Know the types of attacks on aviation
- Know why aviation is an attractive target
- Know how to escort temporary pass holders

The Assessment will be completed on-line via the GPA Redkite System and will consist of 20 random, multiple choice questions. To successfully pass the assessment the applicant must answer a minimum of 18 correctly (90%). The applicant will be allowed a maximum of 3 attempts to successfully complete the Assessment, after which time they will be locked out. If an applicant is locked out of the training, the AS (or their Line Manager) should contact the GPA Security ID Unit.

11.3 How the Applicant will Access ASAT and GSAT

Access to both ASAT and GSAT (alongside the corresponding Assessments) will be provided by the GPA Security ID Unit.

Once the AS is satisfied all elements of the applicant's Standard Background Check have been successfully completed, they should e-mail the following information to Security ID Unit on securityidunit@glasgowprestwick.com:

- The company/participant organisation name
- The applicant's full name
- The applicant's job title
- An e-mail address for the applicant

The Security ID Unit will then e-mail the applicant the link on the GPA Website to complete the ASAT and GSAT E-Learning. They will also register the applicant on the GPA Redkite System and send the applicant their individual User Name and Password to complete the corresponding assessments.

12 SUBMITTING THE AIC APPLICATION TO THE GPA SECURITY ID UNIT

It is important that the Authorised Signatory is both satisfied and assures the GPA Security ID Unit that the Standard Background Check has been completed to the standard detailed in this Guidance before completing and submitting the relevant Application Form to the Security ID Unit.

Before an AIC application is submitted, the Authorised Signatory must review the full referencing pack again for any anomalies or adverse information that may have come to light:

- Has the person's identity been verified through original documents?
- Where appropriate, does the applicant have a right to work in the UK?
- Has a valid and genuine criminal record certificate(s) been obtained and examined for any Disqualifying Convictions?
- Do employment, education or period in receipt of benefit references come from legitimate sources and do they appear genuine?
- Where an applicant has provided the referee contact details, has the AS verified the authenticity of the referee and the subsequent references provided?
- Do all the dates align so there is documentary evidence to cover the full 5-year period with no gaps over 28 days?
- Where a Gap/Personal reference has been provided, is there evidence to show how the person knew what the person has been doing and is there also other supporting evidence?
- Is the content of the references consistent with information supplied by the applicant?
- Is there a legitimate and operational need for the airside access being requested?
- Has the time taken to complete the relevant Background Checks and submit the AIC Application Form to the Security ID Unit resulted in a gap of over 28 days in the referencing history?

At this stage, any remaining exceptional discrepancies or anomalies found must be followed up with the applicant. This should be done in a sensitive manner- there may be a reasonable explanation for apparent inconsistencies. A file-note of any conversation should be made and kept with the applicant's file.

If there is any suspicion of fraudulent activity the matter should be escalated in line with the company/participant organisation's procedures. The AS must notify the company/participant organisation's Nominated Officer (NO) so consideration can be given to alerting the Police or other agency e.g., Border Force. In all instances, the GPA Security ID Unit are available for advice.

12.1 Sending the Application Pack to the GPA Security ID Unit

Once the AS is satisfied everything is in order they should:

- Fully complete Form IDPS 04 - AIC (non-SRA) Application **or** IDPS 05 – AIC (SRA) Application with all the information required. If the AS completes the Application Form with any false information, they will be committing a criminal offence under the Aviation Security Act 1982 (as amended by the Aviation and Maritime Security Act 1990) and may be liable to prosecution

- Send the completed Application Form and supporting paperwork securely to the GPA Security ID Unit – it should **not** be given to the applicant to deliver. The full postal address is: GPA Security ID Unit, Aviation House, Prestwick. KA9 2PL. Alternatively, the completed Application Form and supporting paperwork can be scanned and e-mailed to securityidunit@glasgowprestwick.com as long as the GPA Security ID Unit has a sample copy of the AS's signature and it comes directly from their e-mail account. The supporting paperwork must include:
    - A copy of the New Starter Face-to-Face Security Interview Form (or equivalent)
    - A copy of the identity document(s) checked – the AS must write on the copy 'Original Seen' and sign/date underneath.
    - A copy of the Criminal Record Certificate(s) - the AS must write on the copy 'Original Seen' and sign/date underneath.

- All original references used to support the 5-year history including any supporting evidence obtained and file notes

- Phone (or ask the applicant to phone) the GPA Security ID Unit on 01292 511043 to make an appointment for the issue of the AIC ensuring there will be at least 48 hours between when the GPA Security ID Unit will receive the completed Application Form and the appointment. **NB:** If the application is for an AIC (SRA) there will need to be at least 7 calendar days between when the GPA Security ID Unit will receive the completed Application Form and the appointment to allow time for the Accreditation Check to be requested.

- Tell the applicant they must bring photo ID (valid Passport or Photo Driving Licence) to the appointment with the GPA Security ID Unit to issue the AIC. If the applicant forgets to bring valid photo ID to the appointment, the AIC cannot be issued – they will need to make another appointment

12.2 GPA Security ID Unit Quality Assurance Checks Prior to Issue of AIC

Prior to the issue of an AIC the GPA Security ID Unit will inspect 100% of applicant packs for completeness and to ensure that everything submitted by the AS is fully compliant with all regulatory and GPA policy requirements. This will include:

- Has the face-to-face security interview been conducted, and the appropriate declarations been signed and dated by the applicant and AS?
- Have all parts of the applicant form been completed?
- Has the applicant provided their full name, date of birth and current address?
- Has the AS confirmed that they have checked the applicant's identity?
- Has the AS confirmed they have obtained a CRC? Is this dated within 10 weeks of AIC issue date?
- Have references been provided for the full 5-year period in chronological order?
- If there are any gaps over 28 days between periods of employment, education or in receipt of benefit, are they supported by Gap/Personal references and other supporting evidence?
- Has the AS provided justification for the airside areas to which access is requested?
- Has the applicant successfully completed the mandatory training?

In addition, the GPA Security ID Unit will randomly select a minimum of 10% of applications for further scrutiny and take reasonable steps to verify the validity of the information provided to ensure the quality/accuracy of the background checks conducted by the AS. This will include:

- Reviewing all the references within the application pack with a sceptical eye:
  - Does the employment history look credible when considered as a whole?
  - What's the quality of the reference itself in terms of style, presentation and accuracy?
  - Is there any supporting evidence provided by the AS to corroborate content in the references such as a file note?
- Select and conduct at least one of the following additional checks:
  - Verify the identity of the referees – using internet tools
  - Telephone a selection of referees and check out different facts
  - Check the applicant's online presence
  - Telephone the applicant

If any anomalies or unresolved issues are identified, the nature of any further action will depend upon the specific circumstances and may involve one or more of the following options:

- Making further enquiries with the AS while holding onto the application pack
- Rejecting the applicant and returning all documents to the AS with an explanatory note
- Asking the AS to attend a face-to-face interview

- Contacting the NO of the participant organisation concerned
- Alerting the Police or other agency e.g., Border Force

If, during Quality Assurance Checks, the GPA Security ID Unit repeatedly find poor quality application packs from an AS, a Compliance Audit may be considered appropriate – see Part 19

12.3 Action by GPA Security ID Unit when Issuing the AIC

The checks completed at the point of pass issue play an important part in making sure that an imposter does not present themselves as the real applicant and obtains an AIC by deception.

When the applicant attends the appointment to be issued with their AIC, the GPA Security ID Unit will:

- Inspect the photo identity document the applicant provides (Passport or UK Photo Driving Licence), ensuring the name and date of birth matches the application form and the photo is a likeness of the person standing in front of them
- Confirm the application process has been completed and authorisation to issue has been granted
- Where appropriate, question the applicant regarding their role and/or training to ensure there is a legitimate operational need to access airside
- Take the payment for the AIC – see Part 2.3
- Take a digital photo of the applicant to print on their AIC
- Brief the applicant on their responsibilities as an AIC Holder and issue them with the GPA AIC Holder Conditions of Use Factsheet
- Issue the AIC

Once the AIC has been issued to the applicant, the GPA Security ID Unit will retain the completed Application Form and return the other documents to the AS.

13 RECORD KEEPING FOR AUDIT PURPOSES

In all cases, when returned by the GPA Security ID Unit, the AS must retain a record of the background checks conducted on any AIC applications they have approved. This includes copies of the identity document checked and the criminal record certificates alongside all original references used to support the 5-year history, any supporting evidence obtained and any file-notes in respect of the application. These should be retained for the duration of the persons employment.

Whichever method is used for storage, these records must be accessible to GPA and/or the CAA if needed for Audit purposes.

The company/participant organisation must also ensure they comply with all data protection regulations.

14 AIC AND TEMPORARY PASS HOLDER RESPONSIBILITIES

It is the responsibility of the AS to ensure all AIC and Temporary Pass holders are made aware of their personal responsibilities with regards to the proper use of an AIC or Temporary Pass and the conditions upon which the pass has been issued. This includes their own participant organisations specific conditions.

The AIC or Temporary Pass must only be used by employees (or visitors) for your participant organisation in respect of the client contract submitted as part of your membership of GPA ID Pass Scheme.

If the AIC or Temporary Pass holder transfers or wishes to work for another participant organisation at GPA, a new/second pass must be obtained. AICs and Temporary Passes are not transferable.

The AIC or Temporary Pass must:

- **NEVER** be used by anyone other than the AIC or Temporary Pass holder
- Only be used in connection with the holder's employment for the approver participant organisation and **not for personal reasons**
- Be shown to GPA Security for a visual and or electronic check when entering the Security Restricted Area
- Be kept visible whilst on GPA property and worn at chest height (either with an approved lanyard or arm band)
- Be shown on demand to any compliance authority personnel or any official at GPA, who may need to check that the holder is allowed to be in that area.

The AIC or Temporary Pass Holders responsibilities:

- Safeguard their AIC or Temporary Pass and ensure it is only used by them.
- Understand, if they give their AIC or Temporary Pass for use by another person, it will immediately be revoked and NOT reissued irrespective of how this may affect their employment
- For Temporary Pass holders – remain with their designated Escort at all times
- For AIC holders - ensure that the photograph on the AIC reflects their current appearance.
- Familiarise themselves with the access levels they have been granted - rights can be established by looking at the colour and numbering on the AIC or Temporary Pass
- Co-operate with any security checks
- Remove AICs or Temporary Passes when transiting to and from work. It should not be displayed whilst off-duty, whether in a physical or digital environment.
- Inform the AS if there are any changes to their personal details i.e., name, job title, address.
- Notify the AS (and employer HR department) within 14 days if charged with or convicted of a criminal offence.
- Report any lost or stolen AICs immediately upon discovery to the Airport Police (01292 511234 or 101) and the GPA Security ID Unit (Tel: 01292 511143) or on-shift Airport Security Supervisor (Tel: 01292 511316)
- Where appropriate, challenge and report anyone who is not displaying an AIC or Temporary Pass in a non-public area or any attempted or actual tailgating by individuals
- Challenge and report to GPA Security or Line Manager immediately an unescorted Temporary Pass holder that is airside.
- Must not abuse access privileges to access non-public areas without an express business purpose or to meet, greet or escort family, friends or colleagues in airside areas
- If travelling as a flight passenger, do not use their AIC to by-pass immigration. They must follow standard Border Force protocols and be cleared as an arriving passenger
- Do not prop open security gates/ doors at any time
- Immediately report any observations of suspicious behaviour to their Line Manager, Police or Airport Security
- Report to their Line Manager or Airport Security if they suspect insider threat/behaviour
- Return the AIC or Temporary Pass to the issuer when they leave GPA

15 ON-GOING AIC MONITORING MEASURES

It is important that steps are taken to ensure that all AICs issued are only active when there is an ongoing legitimate operational need. If a participant organisation fails to notify the Security ID Unit that an AIC holder has left their participant organisation, there is a risk that a person could continue to use their existing AIC until it expires. This would result in an AIC being used to access areas/other airports to which they are no longer authorised.

AICs that are no longer required for the purpose they were issued, must be return to the GPA Security ID Unit for cancellation and destruction even if they have expired. From 1st January 2022, a charge will be levied against the participant organisation for all AICs that are not returned.

There are a number of AIC on-going monitoring measures in place to ensure that AICs are only active where there is an ongoing legitimate operational need.

15.1 Suspension of AIC After 60 Days of Inactivity

If an AIC has not been used on-site for 60 calendar days, the GPA Security ID Unit will suspend the AIC and notify the AS by e-mail. The AS will be asked to provide an explanation as to why the AIC has not been used for 60 days, obtain an assurance that there is an on-going operational requirement for the AIC and that the AIC holder has been continuously employed by them during the period of inactivity.

On-going operational requirement and the AIC holder has been continuously employed by the approving participant organisation – the GPA Security ID Unit will re-instate the AIC and ask the holder to swipe a door/gate access to register activity again. If this is not possible, the AIC can only be re-instated when the AIC holder is back on site. A charge is levied for all re-activated AICs.

AIC is no longer required – the GPA Security ID Unit will cancel the AIC and ask the AS to obtain the AIC and return it to the GPA Security ID Unit for destruction. If the AS cannot obtain the AIC, they should provide an explanation for non-return. From 1st January 2022, a charge will be levied against the participant organisation for all AICs that are not returned.

15.2 Requirement to Complete GSAT Training After 6 Months of Inactivity

When an AIC continues to be suspended due to inactivity as per 15.1 above, and the period of suspension reaches 6 months or more, the AIC holder must complete the General Security Awareness Training (GSAT) again before their AIC will be re-activated when they are back on-site.

15.3 Cancellation of AIC After 12 Months of Inactivity

If an AIC has not been used on-site for 12 months, the GPA Security ID Unit will cancel the AIC and notify the AS by e-mail, asking them to obtain the AIC and return it to the GPA Security ID Unit for destruction. If the AS cannot obtain the AIC, they should provide an explanation for non-return. From 1st January 2022, a charge will be levied against the participant organisation for all AICs that are not returned.

This will apply in circumstances where an AIC has been continuously suspended for a 12 month period as per 15.1 above. Cancellation is appropriate at this stage because a legitimate operational need can no longer be justified if the AIC holder has not been on-site for 12 months.

However, in exceptional circumstances only, the period of inactivity before cancellation may be extended to a maximum of 18 months at the discretion of the Security Operations Manager i.e., the AIC holder has been on long-term sickness absence and is due to return to work soon.

15.4 Return of Expired AICs

All AICs that reach their expiry date must be returned to the GPA Security ID Unit for destruction.

The GPA Security ID Unit will notify the AS of any expired AICs that have not been returned, asking them to obtain the AIC and return it to the GPA Security ID Unit. If the AS cannot obtain the AIC, they should provide an explanation for non-return. From 1st January 2022, a charge will be levied against the participant organisation for all AICs that are not returned.

15.5 Annual Review of all AIC Holders

All active AIC holders must be reviewed by the participant organisation on an annual basis to ensure the personal details held by GPA are correct and there is still a legitimate operational requirement for the access permissions granted.

The GPA Security ID Unit will send this list to the AS every 12 months and ask the AS to respond within 10 working days.

15.6 AICs Due for Renewal

A list of all AICs due for renewal in 60 days will be sent to the AS on a weekly basis by the GPA Security ID Unit, however, the AS should be maintaining their own records of AICs issued. The AS should start the renewal action i.e., obtain a new Criminal Records Check Certificate, etc., promptly to avoid a situation where the current AIC expires and there is insufficient information to issue a renewal AIC. See Part 17 on the action required to renew an AIC.

16 AIC - CHANGE MANAGEMENT RESPONSIBILITIES

The participant organisation is responsible for notifying the GPA Security ID Unit of the following changes in a timely manner using Form IDPS 11 - AIC Notification of Changes

This will normally be done by the Authorised Signatory (AS); however, it can also be done by the Nominated Officer (NO) or Line Manager.

16.1 Change in AIC Holders Name – New AIC Must Be Issued

When an AIC holder changes their name, the AS will need to verify this change by sight of valid photo ID (Passport or Photo Driving Licence). If valid photo ID is not available, one of the following must be provided by the AIC holder:

- For a marriage, the original Marriage Certificate
- For civil partners, the original Civil Partnership Certificate

If the AIC holder has gone back to their maiden or unmarried name:

- A Birth Certificate; and
- A signed statement from the AIC holder saying that they have gone back to their Maiden name for all purposes; and
- A Decree Absolute showing both names if the person has divorced; or
- A Marriage Certificate showing both names

If the change of name also includes a change in gender, the AS can also accept one of the following:

- A letter from a doctor or chartered psychologist who practices in gender dysphoria stating that the person has a need to live in a different gender, and evidence of the persons change of name e.g., Deed Poll; or
- A gender recognition certificate; or
- A new birth certificate

The AS must then complete Form IDPS 11 - AIC Notification of Changes and send it, alongside a copy of the relevant documents used to verify the name change, to the GPA Security ID Unit. This can be securely e-mailed to securityidunit@glasgowprestwick.com

The AIC holder should then be advised to phone and make an appointment with the GPA Security ID Unit for the issue of a new AIC. The AIC holder must bring their existing AIC and photo ID (Passport or Photo Driving Licence) to the appointment. The new AIC issued will expire on the same date as the existing AIC. A charge is levied for the issue of a new AIC due to a name change.

16.2 Change in AIC Holders Address and/or Contact Details

When an AIC holder changes their address and/or contact details (phone number or e-mail address), the AS must complete Form IDPS 11 - AIC Notification of Changes and send it to the GPA Security ID Unit. This can be securely e-mailed to securityidunit@glasgowprestwick.com

A new AIC is not required; however, the GPA Security ID Pass Unit must keep the AIC holders address and/or contact details up-to-date on the access control system.

16.3 Change in the AIC Holders Job Role

When an AIC holder changes their Job Role, the AS must complete Form IDPS 11 - AIC Notification of Changes and send it to the GPA Security ID Unit. This can be securely e-mailed to securityidunit@glasgowprestwick.com

The AS will need to indicate on Form IDPS 11 - AIC Notification of Changes if the change in Job Role results in a change in existing Access Permissions. See 16.5 below AIC Holder Needs Changes to Access Permissions.

16.4 AIC Holder Leaves or Changes Employer – Existing AIC Must Be Returned

If an existing AIC holder leaves the approving participant organisation's employment, the AS must complete Form IDPS 11 - AIC Notification of Changes, send it to the GPA Security ID Unit and ensure the AIC is returned to the GPA Security ID Unit immediately for destruction.

If an existing AIC holder ceases to be employed by the approving participant organisation and starts work with another participant organisation (who is also member of the GPA ID Pass Scheme), the AS must still complete Form IDPS 11 - AIC Notification of Changes, send it to the GPA Security ID Unit and ensure the existing AIC is returned to the GPA Security ID Unit immediately for destruction.

The new participant organisation must make a new application for an AIC.

If existing AIC holders are transferring to a new participant organisation under the Transfer of Undertakings Protection of Employment Regulations 1981 (TUPE), the GPA Security ID Unit will support the new participant organisation to facilitate a smooth transition.

16.5 AIC Holder Needs Changes to Access Permissions

When an AIC is issued, Access Permissions will normally be allocated as per the 'Core' permissions agreed for that participant organisation/job role.

If an existing AIC holder needs changes to their Access Permissions at GPA, the process is dependent on whether the change requires a different type of AIC.

A straightforward change i.e., there is no change to type of AIC held, can be done by the AS (or Line Manager) completing Form IDPS 11 - AIC Notification of Changes and sending it to the GPA Security ID Unit explaining the new access permissions required, the duration they are required and reason they are required. This can be securely e-mailed to securityidunit@glasgowprestwick.com

However, if the change in access permissions needed means a change in the type of AIC held (or SRA areas to be accessed) the process will be less straightforward.

Type of AIC Held	Change Needed	Type of AIC Now Needed	Action Required By AS	Action Required By ID Unit
AIC (Non-SRA)	Access to parts of the SRA now required	AIC (SRA)	Completes new application form as Enhanced Background Check now required	As per new AIC (SRA) application process
AIC (SRA) +Area Specific (1-7)	Access to additional parts of the SRA now required	AIC (SRA) +Area Specific (1-7)	Complete Changes Form, send to the ID Unit and advise AIC holder to make appointment for issue of new AIC	Issue a new AIC (SRA) showing new Area(s) for the remaining duration
AIC (SRA) +Area Specific	Access to the SRA no longer required	AIC (Non-SRA)	Complete Changes Form, send to the ID Unit and	This will depend on issue date of previous

Type of AIC Held	Change Needed	Type of AIC Now Needed	Action Required By AS	Action Required By ID Unit
(1-7)			advise AIC holder to make appointment for issue of new AIC	AIC. Remaining duration can only be a max of 3-years from issue date. A new AIC application may be required

16.6 Lost or stolen AIC or Temp Pass

If an AIC or Temp Pass is lost or stolen, immediately upon discovery, the holder must verbally report this to the Airport Police and the GPA Security ID Unit (or on-shift Security Supervisor if the ID Unit is closed) so it can be cancelled on the access control system if necessary.

The AS must then complete Form IDPS 10 – Report of Lost or Stolen AIC and send it to the GPA Security ID Unit for a replacement to be issued. It can be e-mailed to securityidunit@glasgowprestwick.com. A charge is levied for the replacement of lost or stolen AICs.

The AIC holder should then make an appointment with the GPA Security ID Unit for the replacement AIC/Temp Pass to be issued. The holder must bring valid photographic ID (Passport or Photo Driving Licence) to collect the replacement AIC/Temp Pass.

AIC that are subsequently recovered must be returned to the Security ID Unit.

16.7 Extended Periods Not at Work

There may be instances when an AIC holder may not have an operational business need to access GPA for extended periods, for example, due to:

- An on-going investigation; or
- A period of extended unpaid leave; or
- Maternity/ paternity leave; or
- A career break; or
- A sabbatical; or
- Seasonal employee

In these cases, the AS is obligated to notify the GPA Security ID Unit to suspend the AIC when the investigation or work break commences giving the reasons. The AS must complete Form IDPS 11 - AIC Notification of Changes and send it to the GPA Security ID Unit. This can be securely e-mailed to securityidunit@glasgowprestwick.com

The AS should also withdraw the AIC from the holder and store it securely until they return to work. If the AIC is due to expire before their return to work date, it should be returned to the GPA Security ID Unit.

When the AIC holder returns to work, the AS should contact the GPA Security ID Unit to ask for the AIC to be re-instated. If the break has lasted 6 months or more, the AIC holder will need to complete GSAT again before the AIC can be re-instated. A charge will not be levied to re-instate the AIC as long as the GPA Security ID Unit was notified of the extended break from work when it started.

If the AIC has expired more than 28 days before their return to work, a new AIC application will need to be made. If the AIC has expired less than 28 days before their return to work, a renewal AIC application can be made.

17 RENEWING AN AIC PRIOR TO EXPIRY

An AIC can be renewed on expiry as long as there is still a legitimate operational need for the AIC.

However, it's very important, the action needed to apply for a renewal AIC, is started at least 60 days prior to the expiry of the existing AIC to make sure there is no interruption to the AIC holder's airside access.

17.1 Renewal of AIC (Non-SRA) and AIC (SRA)

A Standard Background Check (non SRA access) or Enhanced Background Check (SRA access), alongside the mandatory training must be completed again prior to the issue of a renewal AIC.

This means, at least 60 days before expiry of an AIC, the AS should start the renewal process by:

1. Verifying the renewal applicant has not changed their identity – this is normally a recent copy of their photo ID (Passport or Photo Driving Licence); **and**

2. Obtain a new Criminal Records Check Certificate (Basic Disclosure) dated within 10 weeks of the renewal AIC issue date to confirm the renewal applicant still has no disqualifying convictions– see Parts 7.3 to 7.5; **and**

3. Obtain a reference from an authorised person in the participant organisation confirming the renewal applicant has been continuously employed with them since the date the expiring AIC was issued. NB: as long as a renewal application is made no more than 28-days after the existing AIC expiry, no further references will be required. If the existing AIC expired more than 28 days ago, a full application is required.

4. Confirm the renewal applicant has successfully completed ASAT and GSAT training again – see Part 11.

5. Confirm there is still a legitimate operational need for the renewal applicant's current access permissions.

6. Fully complete Form IDPS 08 or IDPS 09 (see below).

17.2 Sending the Renewal AIC Application Pack to the GPA Security ID Unit

Once the AS is satisfied everything is in order they should:

- Fully complete Form IDPS 08 - AIC (non-SRA) Renewal Application or Form IDPS 09 – AIC (SRA) Renewal Application with all the information required. If the AS completes Renewal Application Form with any false information, they will be committing a criminal offence under the Aviation Security Act 1982 (as amended by the Aviation and Maritime Security Act 1990) and may be liable to prosecution

- Send the completed Renewal Application Form and supporting paperwork securely to the GPA Security ID Unit – this should not be given to the applicant to deliver. The full postal address is: GPA Security ID Unit, Aviation House, Prestwick. KA9 2PL. Alternatively, the completed Renewal Application Form and supporting paperwork can be scanned and e-mailed to securityidunit@glasgowprestwick.com as long as the GPA Security ID Unit has a sample copy of the AS's signature and it comes directly from their e-mail account. The supporting paperwork must include:
  - A copy of the identity document(s) checked
  - A copy of the new Criminal Record Certificate(s)
  - The reference to confirm the renewal applicant has been continuously employed since the date the expiring AIC was issued

- Phone (or ask the renewal applicant to phone) the GPA Security ID Unit on 01292 511043 to make an appointment for the issue of the renewal AIC ensuring there will be at least 48 hours between when the GPA Security ID Unit will receive the completed Renewal Application Form and the appointment. **NB:** If the renewal application is for an AIC (SRA) there will need to be at least 7 calendar days between when the GPA Security ID Unit will receive the completed Application Form and the appointment to allow time for the Accreditation Check to be requested.

- Tell the renewal applicant they must bring their existing AIC and photo ID (valid Passport or Photo Driving Licence) to the appointment with the GPA Security ID Unit to issue the AIC. If the applicant forgets to bring their existing AIC or valid photo ID to the appointment, the renewal AIC cannot be issued – they will need to make another appointment

17.3 GPA Security ID Unit Quality Assurance Checks Prior to Issue of a Renewal AIC

Prior to the issue of a renewal AIC the GPA Security ID Unit will inspect 100% of renewal applicant packs for completeness and to ensure that everything submitted by the AS is fully compliant with all regulatory and GPA policy requirements. This will include:

- Have all parts of the renewal applicant form been completed?
- Has the AS confirmed that there has been no change in the applicant's identity?
- Has the AS confirmed they have obtained another CRC? Is this dated within 10 weeks of renewal AIC issue date?
- Has a reference been supplied to confirm continuous employment by the participant organisation since the date the expiring AIC was issued?
- Has the renewal application been made no more than 28-days after the existing AIC expires?
- Has the AS provided confirmation the same access permissions are still needed?
- Has the applicant successfully completed the mandatory training again?

In addition, the GPA Security ID Unit will randomly select a minimum 10% of renewal applications for further scrutiny and take reasonable steps to verify the validity of the information provided to ensure the quality/accuracy of the renewal background checks conducted by the AS. This will include:

- Reviewing all the references within the application pack with a sceptical eye:
    - Does the employment history look credible when considered as a whole?
    - What's the quality of the reference itself in terms of style, presentation and accuracy?
    - Is there any supporting evidence provided by the AS to corroborate content in the references such as a file note?
- Select and conduct at least one of the following additional checks:
    - Verify the identity of the referees – using internet tools
    - Telephone a selection of referees and check out different facts
    - Check the applicant's online presence
    - Telephone the applicant

If any anomalies or unresolved issues are identified, the nature of any further action will depend upon the specific circumstances and may involve one or more of the following options:

- Making further enquiries with the AS while holding onto the renewal application pack
- Rejecting the renewal applicant and returning all documents to the AS with an explanatory note
- Asking the AS to attend a face-to-face interview
- Contacting the NO of the participant organisation concerned
- Alerting the Police or other agency e.g., Border Force

If, during Quality Assurance Checks, the GPA Security ID Unit repeatedly find poor quality renewal application packs from an AS, a Compliance Audit may be considered appropriate – see Part 19

17.4 Action by GPA Security ID Unit when Issuing the Renewal AIC

The checks completed at the point of pass issue play an important part in making sure that an imposter does not present themselves as the real applicant and obtains a renewal AIC by deception.

When the applicant attends the appointment to be issued with their renewal AIC, the GPA Security ID Unit will:

- Inspect the photo identity document the applicant provides (Passport or UK Photo Driving Licence), ensuring the name and date of birth matches the renewal application form and the photo is a likeness of the person standing in front of them
- Confirm the renewal application process has been completed and authorisation to issue has been granted
- Where appropriate, question the applicant regarding their role and/or training to ensure there is still a legitimate operational need to access airside
- Take the payment for the renewal AIC – see Part 2.3
- Take a digital photo of the applicant to print on their renewal AIC
- Brief the applicant on their responsibilities as an AIC Holder and issue them with the GPA AIC Conditions of Use Factsheet
- Destroy the expiring AIC
- Issue the renewal AIC

Once the renewal AIC has been issued to the applicant, the GPA Security ID Unit will retain the completed Renewal Application Form and return the other documents to the AS.

18 WHEN AN AIC/TEMP PASS MAY BE WITHDRAWN OR CANCELLED

AIC or Temp Pass holders do not have the automatic right to an airside pass even if they meet the criteria and/or it has been issued. The AIC or Temp Pass remains the property of GPA, who reserve the right to refuse, cancel or withdraw an AIC or Temp Pass in the event of substantial cause or there is doubt raised over the suitability of holder.

Part 16 of this guidance covers Change Management Responsibilities, however, there are other instances when an individual AIC or Temp Pass may be withdrawn or cancelled by the GPA Security Team. This includes, but is not limited to:

- When there has been misrepresentation of the facts when applying for the AIC or Temp Pass; or
- When an AIC holder is convicted of a disqualifying criminal offence; or
- If the AIC or Temp Pass appears to have been falsified or tampered with; or
- The AIC or Temp Pass is being misused – this includes use for non-business reasons or being used by someone other than the holder; or
- The removal is in connection with the detection and/or prevention of crime or a threat to security; or
- Where an AIC holder has their national security clearance suspended; or
- Where there has been a serious breach (or repeated breaches) of safety or security regulations or procedures; or
- Where there is misconduct by the AIC or Temp Pass holder - this may include, but is not limited to:
    - Failing to adhere to security regulations (such as disguising or concealing prohibited items and attempting to bring them airside) or failing to comply with a verbal or written instruction by the GPA Security Team, Police or other airport official; or
    - Not wearing their AIC or Temp Pass in a visible place or failing to show it on demand to a member of the GPA Security Team, Police or other airport official; or
    - Trying to access areas in respect of which they are not authorised to enter; or
    - Facilitating entry to airside areas for other persons/allowing or participating in ‘tailgating’; or
    - Propping open or leaving an access door/gate unsecure; or
    - Intentionally damaging access control equipment or any other airport property; or
    - Threatening or violent behaviour: or
    - Unauthorised use of a vehicle driving airside; or
    - Escorting anyone airside without a temporary pass; or
    - Failure to keep their AIC sponsoring/approving participant organisation and GPA informed of a material change in their personal circumstances i.e., change of name, address, contact details or convicted of a criminal offence

When an AIC or Temp Pass has been withdrawn due to substantial cause or there is doubt raised over the suitability of the holder, the GPA Security Operations Manager will conduct a full assessment before reaching a decision on whether the AIC or Temp Pass should be permanently cancelled.

During this assessment, they will discuss the issues with the AIC sponsoring/approving participant organisation and may ask them to conduct their own internal investigation. The GPA Security Operations Manager will then:

- Consider each case solely on its merits; and
- Clearly record the reasons for the decision arrived at; and
- Notify the AIC/Temp Pass holder and sponsoring/approving participant organisation of their decision; and
- Have a fair and open process for considering appeals

If the GPA Security Operations Manager decided to permanently cancel an AIC or Temp Pass, this may have a significant effect on the holder’s capability to perform their job. Decisions regarding the employee’s status, or terms and conditions, are the employer’s responsibility. GPA will not advise on any action the employer may take, nor get drawn into any discussions around employment matters. In addition, there will be no refund of any charges paid.

19 QUALITY ASSURANCE & COMPLIANCE AUDITS

The GPA Security ID Unit will conduct quality assurance checks of all AIC applications. This includes 100% completeness checks and a random 10% further scrutiny check as detailed at Parts 12.2 and 17.3.

In addition, GPA will conduct full Compliance Audits. These audits may be initiated as a result of errors or omissions identified through the quality assurance checks, however, GPA will aim to audit all participant organisations on a regular basis. In addition, the Civil Aviation Authority (CAA) may include a participant organisation in their independent audits.

A Compliance Audit will cover a wider scope than the quality assurance checks. It may include, but is not limited to:

- Where AIC applications are frequently submitted with errors or omissions, the main aim of the audit will be to:
    - determine the underlying cause for the poor quality applications being submitted; and
    - agree, where appropriate, action to resolve these causes
- Establishing the participant organisations internal procedures used to verify the background of AIC applicants and assessing whether they are in accordance with the GPA ID Pass Scheme Guidance; and
- Explore with the NO and AS their understanding of their security responsibilities and ongoing pass change management procedures i.e., how they ensure all AICs are returned to the GPA Security ID Unit when they are no longer required; and
- A comparison and contrast of all the documents supplied to support each AIC application; and
- Identification of any vulnerabilities or training needs; and
- Evidence that security risks for potential and existing AIC holders are being effectively managed

Where possible, GPA will provide the NO with a minimum 7-days' notice of a Compliance Audit.

19.1 Action following a Compliance Audit

GPA will provide the NO with an audit report detailing the findings. Where appropriate, a rectification action plan will be agreed and maintained until all actions have been completed. If the audit finds significant deficiencies, the participant organisation may be put on Special Measures (see Part 19.2 below).

19.2 Special Measures

If an audit finds significant deficiencies that mean there is a real and serious on-going risk to security, the participant organisation's membership of the GPA ID Pass Scheme may be terminated by GPA (see Part 20). However, as an alternative to immediate termination, special measures may be considered to allow the participant organisation to urgently rectify all areas of non-compliance. The decision on the implementation and duration of special measures will be made by the GPA Security Operations Manager and must be agreed by the participant organisation. Special measures may include, but are not limited to:

- 100% full scrutiny check by the GPA Security ID Unit of all AIC applications – a charge will be levied for all scrutiny checks conducted over the standard 10%; and
- Bi-weekly updates from the participant organisation on progress toward compliance; and
- A further Compliance Audit when the participant organisation has rectified all areas of non-compliance – if this audit still finds non-compliance, the participant organisation's membership of the GPA ID Pass Scheme will be terminated by GPA

20 TERMINATION OF PATICIPATION IN THE GPA ID PASS SCHEME

Both GPA and the participating participant organisation can terminate their membership of the GPA ID Pass Scheme. When membership is terminated, all existing GPA AICs sponsored/approved by the participant organisation must be cancelled and returned to the GPA Security ID Unit. There will be no refund of any charges paid.

20.1 GPA's Right to Terminate Membership

GPA reserves the right to immediately terminate a participant organisations membership of the GPA ID Pass Scheme and suspend or cancel any GPA AICs sponsored/approved by that same participant organisation under the GPA ID Pass Scheme in the event that:

- It is required to do so by operation of a Law, Regulation, or other Legislation applicable in the relevant jurisdiction; or
- There is evidence of impropriety or misconduct by the participant organisation, Nominated Officer or Authorised Signatory in relation to non-compliance with the requirements set out in this Guidance; or
- There is evidence of pervasive misappropriation of GPA AICs throughout the participant organisation i.e., a culture of individuals sharing GPA AICs; or
- The participant organisation has previously had GPA AICs cancelled after 45-days due to non-payment of an invoice and again, fails to pay an invoice within 45-days; or
- The participant organisation is in quantifiable breach of the GPA ID Pass Scheme Terms & Conditions and has failed to alleviate such a breach within 30-days of service of notice to do so by GPA; or
- The participant organisation suffers a change of control or an insolvency event: or
- The participant organisation has not submitted an AIC application for a period of 6-months and there are no existing GPA AICs holders sponsored/approved by that same participant organisation

If GPA terminates a participating participant organisation's membership of the GPA ID Pass Scheme, they will do so in writing to the Nominated Officer. Where possible, GPA will endeavour to give the participating participant organisation a minimum of 30-days' notice of termination, however, this may not be possible. In addition, the participating participant organisation must:

- Ensure all existing GPA AICs sponsored/approved by them are returned to the GPA Security ID Unit by the date notified in the letter; and
- Understand the GPA Security ID Unit will cancel all existing GPA AICs sponsored/approved by them on the date notified in the letter; and
- Levy a charge for any GPA AICs sponsored/approved by then that are not returned to the GPA Security ID Unit within 20-days of the date notified in the letter; and
- Pay any outstanding charges within 14-days of receipt of the final invoice

20.2 Participant Organisation's Right to Terminate Membership

A participant organisation has the right to terminate its membership of the GPA ID Pass Scheme. The request must be made in writing to the GPA Security ID Unit. In addition:

- The participant organisation must give GPA a minimum of 30-days' notice that they want to end their membership of the GPA ID Pass Scheme; and

- The participant organisation must ensure all existing GPA AICs sponsored/approved by them are returned to the GPA Security ID Unit by the end of the notice period; and
- The GPA Security ID Unit will cancel all existing GPA AICs sponsored/approved by them at the end of the notice period and levy a charge for any GPA AICs not returned with 20-days of the termination date; and
- The participant organisation will pay any outstanding charges within 14-days of receipt of the final invoice

21 APPEALS

A participant organisation can Appeal the following GPA decisions only:

- Rejection of a Participant organisations Application to Join the GPA ID Pass Scheme
- Rejection of a new or renewal Application for a GPA AIC
- Rejection of a new or renewal Application for a TVP(SRA) or TEP(SRA)
- Withdrawal or Cancellation of an GPA AIC
- Withdrawal or Cancellation of a TVP(SRA) or TEP(SRA)
- Termination of a Participant Organisations Membership of the GPA ID Pass Scheme

Any appeal must be made in writing within 30-days of the decision notification, made in accordance with the GPA ID Pass Scheme Terms & Conditions and contain a full explanation of why the participant organisation disagrees with the decision. Any supporting evidence should also be included.

Any appeal should be sent to:

Jules Matteoni
Operations Director
Glasgow Prestwick Airport
Aviation House
Prestwick
KA9 2PL

E-Mail: jmatteoni@glasgowprestwick.com

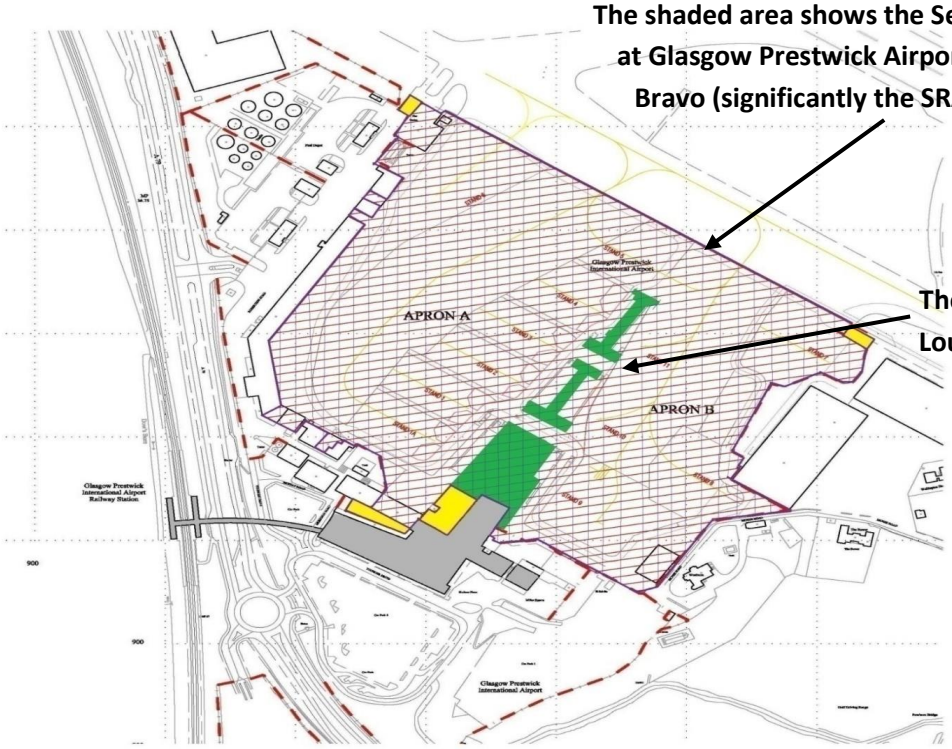
GPA will endeavour to respond to all Appeals within 30-days of receipt.

22 Annex 1 - GPA SECURITY RESTRICTED AREA (SRA)

Number	SRA Access Area
1	Internal Area (Departure Lounge)
2	Baggage Re-claim Hall
3	Baggage Make-Up Area
4	Ramp
5	Aircraft and their Footprints
6	*Not used by GPA*
7	All areas of the SRA

The shaded area shows the Security Restricted Area (SRA) at Glasgow Prestwick Airport, Apron Alpha and Apron Bravo (significantly the SRA is also the Critical Part)

The Forward Finger and Departure Lounge are also in the SRA and are highlighted in Green



GLASGOW PRESTWICK AIRPORT
Restricted Zone
Glasgow Prestwick Airport
24.08.07
1: 2500 @ A3
J: Projects/Q/998/100
Q/998/100

23 Annex 2 - GPA ID PASS SCHEME CHARGES

The participant organisation will pay the following charges that apply to services provided under the GPA ID Pass Scheme.

Payment by credit/debit card is due to the GPA Security ID Unit at the point of delivery. Cash in not accepted. When agreed in advance, invoices may be sent to the participant via the GPA Accounts Department, detailing the exact cost of each service provided and must be paid within 14-days.

Cost – *Effective 1st October 2022	**Cost – Excluding VAT**	**VAT @ 20%**	**Cost – Including VAT**
Initial/Renewal 3-Year Airside AIC	£83.33	£16.67	£100.00
Initial/Renewal 5-Year Airside AIC (with SRA)	£91.67	£18.33	£110.00
Accreditation Check ONLY – will normally be included in the cost of Airside AIC (with SRA)	£25.00	£5.00	£30.00
Initial/Renewal 3-Year Landside Only AIC	-	-	-
Airside Safety Awareness Training (as required)	Included in cost of AIC	Included in cost of AIC	Included in cost of AIC
General Security Awareness Training (as required)	Included in cost of AIC	Included in cost of AIC	Included in cost of AIC
Lost/Stolen AIC – Replacement AIC Required	£37.50	£7.50	£45.00
Authorised Signatory Action – Initial (as agreed by GPA)	£200.00	£40.00	£240.00
Authorised Signatory Action – Renewal (as agreed by GPA)	£75.00	£15.00	£90.00
Damaged AIC – Replacement AIC Required	£37.50	£7.50	£45.00
Reactivation of a Suspended AIC	£20.83	£4.17	£25.00
Amend Personal/Participant details – New AIC Required	£29.17	£5.83	£35.00
Administrative Charge due to Legislation Change – New AIC Required	£20.83	£4.17	£25.00
Temporary Employment Pass (TEP) to CP-SRA	£29.17	£5.83	£35.00
Temporary Visitor Pass (TVP) to CP-SRA	-	-	-
Special Measures - Additional Scrutiny Checks (over 10%) per AIC Holder	£41.67	£8.33	£50.00
AIC not returned within 30 days of invalidity or expiry	£41.67	£8.33	£50.00

***Costs are subject to regular review. Participant organisations will be given 30-day's notice of any changes.**