



QUALITY MANUALS | FIRST EDITION

IAF INDUSTRIAL FACILITY SECURITY AND REVERSE ENGINEERING PROTECTION MANUAL

Facility access control and
engineering information protection

STABLE RELEASE

Document No. IAF-MAN-ISP-001 | Revision 01

Visitors contractors and third party access
Research assets and production information
Security incidents and evidence preservation

International Automotive Federation

English master text | 15 September 2026

iaf.com

Publication identity and use

IAF Industrial Facility Security and Reverse Engineering Protection Manual

This manual establishes protective controls for automotive factories, research centres, pilot workshops and connected engineering environments. It governs visitors, suppliers and contractors, protects confidential designs and production knowledge, and defines proportionate responses to unauthorised acquisition, disclosure or interference with industrial assets.

Control	Publication record
Document	IAF-MAN-ISP-001 IAF Industrial Facility Security and Reverse Engineering Protection Manual
Edition and revision	First Edition Revision 01 Stable Release
Text issue	15 September 2026 English master text
Document owner	IAF Quality function and the relevant automotive technical committee
Custodian	IAF Secretariat and Document Controller
Institutional authority	Competent authority under IAF-CON-001. Publication does not amend the Constitution.
Operational adoption	Accountable operating director and competent technical leads record the actual approval, markets, scope and effective date.
Classification	Public core manual. Completed operational, technical and security records follow their assigned access controls.

Application of requirements

“Shall” identifies a requirement when this manual is adopted by an organisation or agreement. “Should” identifies a recommendation. Worked examples are illustrative and supply no universal legal deadline, product limit or completed approval. Annexes provide record structures for controlled local implementation.

Publication and operational release

Stable Release identifies the completed publication text. Actual operating approvals, market obligations, technical validation and role authorisations shall be established by the responsible organisation. Mandatory law, applicable customer rights, approved product requirements and safe work instructions remain controlling for the specific operation.

IAF recognition

Using this manual does not itself confer membership, Corporate Recognised status, accreditation, certification or permission to use IAF marks. Those decisions follow the applicable IAF guides, independent evaluation and recorded scope.

Contents

Entries link to their sections and include the cover in page numbering.

1 Purpose and protective outcomes	7
2 Terms and asset boundaries	8
3 Governance and separation of responsibilities	9
4 Operational adoption and lawful controls	10
5 Asset inventory and ownership	11
6 Information classification and handling	12
7 Threat and vulnerability assessment	13
8 Security zoning and access boundaries	14
9 Perimeter control and life safety	15
10 Identity verification and preauthorisation	16
11 Visitor arrival and departure procedure	17
12 Sponsorship escort and hosted activities	18
13 Contractor engagement and work authorisation	19
14 Work boundaries and change permits	20
15 Subcontractors and personnel substitution	21

Contents continued 2

Entries link to their sections and include the cover in page numbering.

16 Onboarding transfer and offboarding	22
17 Badges keys and access reviews	23
18 Restricted research and development areas	24
19 Production cells and process knowledge	25
20 Prototypes models and unreleased vehicles	26
21 Tooling additive files and controlled scrap	27
22 Photography recording and personal devices	28
23 Meetings displays and technical demonstrations	29
24 Deliveries drivers and loading areas	30
25 Secure transport and offsite custody	31
26 Samples loans and external technical work	32
27 Digital identities and least privilege	33
28 Engineering repositories and version integrity	34
29 External collaboration and technical data sharing	35
30 Remote support and operational technology access	36

Contents continued 3

Entries link to their sections and include the cover in page numbering.

31 Removable media and portable equipment	37
32 Machine programmes and production backups	38
33 Cloud platforms artificial intelligence and digital twins	39
34 Data loss monitoring and alert handling	40
35 Cameras biometrics and privacy safeguards	41
36 Insider concerns and protected reporting	42
37 Contracts intellectual property and confidentiality	43
38 Reverse engineering protection and lawful boundaries	44
39 Product tamper controls and service access	45
40 Competitive benchmarking and clean separation	46
41 Incident intake and initial triage procedure	47
42 Containment and evidence preservation procedure	48
43 Investigation fairness and disclosure decisions	49
44 Recovery and controlled restoration procedure	50
45 Emergency access and business continuity	51

Contents continued 4

Entries link to their sections and include the cover in page numbering.

46 Competence awareness and scenario exercises	52
47 Audit metrics and management review	53
48 IAF interfaces records and revision control	54
Annex A Adoption asset and zone register	55
Annex B Individual access request and review	56
Annex C Visitor visit and escort record	57
Annex D Contractor work scope and closure	58
Annex E Device photography and publication permission	59
Annex F Technical information sharing record	60
Annex G Prototype tooling and sample custody	61
Annex H Role change and offboarding checklist	62
Annex I Incident and evidence custody record	63
Annex J Monitoring and privacy assessment	64
Annex K Worked access and custody metrics	65
Annex L Contractor disclosure and recovery exercise	66

Using the operational annexes

Create a separate controlled record for each case. Expand the editable worksheets as needed and enter actual values, evidence links, responsible names and dates. Blank fields and worked examples are not proof of a completed activity.

1 Purpose and protective outcomes

1.1 The operating organisation shall protect automotive facilities, research activity and engineering information against unauthorised access, acquisition, disclosure and interference. The protection programme shall cover people, physical assets, technical data and the interfaces between them. Its purpose is to preserve safe operations and legitimate confidential interests while enabling authorised production, collaboration, service and oversight.

1.2 The Security Manager shall define the sites, workshops, laboratories, warehouses, digital environments and third party activities within scope. The programme shall include prototypes, tooling, process knowledge, software, drawings and combinations of information that reveal sensitive design intent. Protection shall follow the asset throughout its lifecycle, including transport, loan, repair, reuse and disposal.

1.3 Controls shall be proportionate to a documented risk assessment and shall have identifiable owners, operating instructions and evidence of effectiveness. A confidentiality label or signed agreement alone shall not be treated as a complete protective system. Physical access and digital permissions shall be coordinated so that an authorised visit does not unintentionally grant unrestricted technical access.

1.4 Security shall support lawful operations and shall not override emergency egress, worker safety, required disclosures, protected reporting or legitimate customer rights. This manual establishes organisational controls; it does not create a universal legal prohibition on reverse engineering or give IAF statutory enforcement powers. Actual rights, restrictions and investigative actions shall be assessed for the relevant jurisdiction and contract.

2 Terms and asset boundaries

2.1 An asset is information, equipment, material, capability or a relationship whose loss or misuse could harm the organisation or another rights holder. An asset owner is the role accountable for classification, authorised use and protection decisions. A custodian operates the controls but does not automatically have authority to expand access or change the permitted purpose.

2.2 Restricted information is information assigned additional controls because of its sensitivity or obligations. A trade secret claim requires a factual and legal assessment of secrecy, value and protective measures; a label alone does not establish the claim. Publicly available information shall not be described as confidential solely to prevent legitimate scrutiny or competition.

2.3 A security zone is an area with defined access conditions, permitted activities and an accountable owner. A visitor is present for a temporary authorised purpose, while a contractor performs a defined service under a controlled scope. Employment by a supplier, possession of a badge or attendance at an earlier visit shall not create continuing access rights.

2.4 An incident is an event or credible indication of unauthorised access, disclosure, loss or interference requiring assessment. A suspicion is not a finding of misconduct. Records shall distinguish observed facts, technical indicators, witness accounts and assumptions, preserving the ability to investigate fairly and correct an initial interpretation when evidence changes.

3 Governance and separation of responsibilities

3.1 The accountable site director shall provide resources and decision authority for the security programme. The Security Manager shall coordinate physical protection, incident response and third party access. Engineering asset owners shall classify technical information and approve its release, while Information Security shall manage digital controls in cooperation with operational technology owners.

3.2 Human Resources shall govern employment related actions, and Legal and Privacy functions shall assess contracts, monitoring, investigation powers and disclosure obligations. Health and Safety shall control emergency and safe work requirements. Security personnel shall not independently change machine safety logic, conduct intrusive personal investigations or impose disciplinary outcomes outside their authorised role.

3.3 Business sponsors shall justify access, supervise the permitted activity and close the engagement. They shall not approve their own exceptions where an independent asset or security decision is required. Purchasing shall ensure that supplier and subcontractor arrangements contain workable access, confidentiality, incident notification and return obligations rather than relying on a general purchase order statement.

3.4 The responsibility matrix shall name deputies and escalation routes for out of hours events. Decisions to restrict access, preserve evidence, notify affected parties or resume activity shall be recorded with their basis. Disputes shall be escalated without allowing commercial pressure to erase a valid protective hold or allowing security concerns to obstruct a required safety action.

4 Operational adoption and lawful controls

4.1 The site director shall adopt this manual for identified facilities, systems and activities after reviewing local legal and operational conditions. The adoption record shall state the effective operating date, accountable roles, required local procedures and implementation gaps. Publication of the manual shall not be represented as proof that all controls are already installed and effective.

4.2 Legal, Privacy, Human Resources and worker consultation functions, where applicable, shall assess controls affecting personal information, searches, monitoring and employment. The organisation shall identify the lawful purpose and limits of each measure. A blanket consent statement or contractual clause shall not be assumed to authorise every form of surveillance, access to personal devices or retention of personal records.

4.3 Local supplements shall define emergency numbers, security contacts, access procedures, restricted zone rules and incident escalation. Sensitive site layouts, system details and response tactics shall be held in controlled records rather than public versions of this manual. Instructions shall remain understandable to contractors and visitors through suitable language and accessible formats.

4.4 Implementation gaps shall have owners, interim controls and closure evidence. The site shall test access controls, egress, alarm response and role handovers before claiming operational readiness. Significant changes to layout, activities, technology or law shall trigger reassessment, with records showing what changed and how affected personnel were informed.

5 Asset inventory and ownership

5.1 Engineering and operational functions shall maintain an inventory of assets requiring protection. The inventory shall include drawings, source code, process recipes, simulation models, digital twins, prototypes, fixtures, test data, manufacturing programmes and confidential commercial information. It shall identify the owner, custodian, location, lifecycle stage, authorised uses and external dependencies.

5.2 The assessment shall consider combinations of otherwise ordinary information that reveal sensitive capabilities, such as a process sequence linked to tolerances and supplier choices. Owners shall identify which elements need restricted access and which can be shared safely. Overclassification shall be challenged where it impedes necessary work without a reasoned protective benefit.

5.3 Assets held by suppliers, testing facilities, cloud providers or logistics partners shall remain visible in the inventory. The organisation shall record custody, contractual rights, return conditions and the evidence needed to verify disposal or deletion. Transfer to another organisation shall not be assumed to remove the original owner's responsibility for deciding the permitted use.

5.4 The inventory shall be reviewed at programme gates, site changes and engagement closure. Obsolete prototypes and abandoned repositories shall receive a deliberate disposition rather than remain unowned. The owner shall preserve records needed for safety, warranty, compliance or legal holds while removing unnecessary access and uncontrolled copies.

6 Information classification and handling

6.1 The organisation shall define a manageable classification scheme, such as Public, Internal, Confidential and Restricted, with clear handling requirements for each level. The asset owner shall assign classification based on disclosure impact, contractual obligations and intended use. Classification shall be visible in the record or system without revealing the sensitive content through an unnecessarily descriptive public filename.

6.2 Handling rules shall address access approval, storage, transmission, printing, copying, meeting use and disposal. Restricted technical data shall use approved repositories and attributable sharing channels. Personal email, uncontrolled messaging and unapproved file transfer services shall not be used to bypass an inconvenient access process.

6.3 Owners shall review classification when information becomes public, a programme closes or contractual obligations change. Downgrading shall require an authorised decision that considers combined information and third party rights. Upgrading shall identify existing recipients and copies so that the new control is implemented in practice rather than applied only to the master file.

6.4 Employees and contractors shall have a practical route to request access or challenge an unclear classification. Training shall use examples from actual work, including drawings displayed on screens, photographs containing background detail and machine backups. A restrictive label shall never be used to hide a safety defect, prevent protected reporting or misrepresent information that must lawfully be disclosed.

7 Threat and vulnerability assessment

7.1 The Security Manager shall coordinate a documented assessment of credible threats, exposed assets and control weaknesses. Scenarios shall include unauthorised photography, stolen credentials, misdirected files, contractor overreach, prototype loss, insider misuse and compromise of engineering or production systems. The assessment shall distinguish likelihood, consequence, existing controls and uncertainty rather than relying on a single unexplained score.

7.2 Evidence shall focus on conduct, access opportunity, technical indicators and known vulnerabilities. Nationality, ethnicity, religion or other protected characteristics shall not be used as a proxy for malicious intent. Business relationships and legal restrictions may require specific checks, but the basis and scope shall be documented and applied lawfully and consistently.

7.3 The team shall examine how physical and digital weaknesses combine, such as an unescorted technician using an unattended engineering workstation. It shall consider accidental disclosure and ordinary process errors alongside deliberate misconduct. Controls shall address the actual pathway, with an owner and a test of effectiveness rather than a broad instruction to remain vigilant.

7.4 Risk acceptance shall be authorised by the accountable owner within defined limits and shall not waive legal or safety requirements. Assessments shall be updated after incidents, major layout changes, new collaboration models or emerging credible threats. Sensitive findings shall be distributed only to roles that need them to implement and verify the protective action.

8 Security zoning and access boundaries

8.1 The site shall define zones according to the sensitivity of activities and the consequences of unauthorised access. Typical distinctions include public reception, general operations, controlled production and restricted research areas. Each zone shall have an owner, entry conditions, permitted activities, escort requirements and a method for revoking access when the purpose ends.

8.2 Zone design shall consider sight lines, noise, displays, waste routes, shared corridors and neighbouring work areas. A barrier around a laboratory may be ineffective if confidential prototypes remain visible from a visitor route. The owner shall identify practical controls for observation and information exposure without obstructing safe movement or creating unnecessary operational hazards.

8.3 Physical permissions shall be linked to work purpose, time and competence where relevant. Access to one zone shall not automatically grant access to adjacent restricted areas or digital systems. Temporary permissions shall expire, and extensions shall require confirmation that the activity and sponsor remain valid.

8.4 The site shall maintain controlled zone maps and verify them against actual doors, signs and access rules. Changes shall be reviewed with Security, Operations and Health and Safety. Emergency egress shall remain compliant and usable, with alarm or monitoring arrangements designed so that protection of information never depends on trapping people inside a restricted area.

9 Perimeter control and life safety

9.1 The site shall assess perimeter protection, reception points, vehicle gates and delivery access against credible risks and operational needs. Controls shall enable authorised entry while detecting or discouraging unauthorised intrusion. Lighting, barriers and observation arrangements shall be maintained and tested without disclosing sensitive weaknesses in public documents.

9.2 Security staff shall verify credentials and purpose using the approved process, with a safe escalation route for discrepancies. They shall not use an unfamiliar person or vehicle as grounds for unsafe confrontation. Suspected intrusion shall be managed through trained response procedures, preserving personal safety and involving public emergency services when the circumstances require their authority.

9.3 Fire exits, evacuation routes and emergency access shall remain available under the applicable safety arrangements. Access control failure modes shall be selected with competent life safety input rather than applying one universal locking rule. Changes to doors, turnstiles or vehicle barriers shall be checked for their effect on evacuation and emergency response.

9.4 Inspection records shall capture defects, temporary controls and repair completion. Power or network loss shall trigger the approved continuity procedure, including controlled manual entry where justified. Temporary arrangements shall have a responsible person, access log and end condition, preventing a short outage from becoming an indefinite unmonitored access route.

10 Identity verification and preauthorisation

10.1 The sponsor shall request access before arrival and identify the person's employer, role, purpose, required zones, dates and systems. Security shall verify identity through a proportionate process and confirm that the request has the necessary approvals. Identity documents shall be viewed or recorded only to the extent justified by applicable requirements and the access risk.

10.2 Preauthorisation shall distinguish the individual from the supplier company. A contract with an organisation shall not automatically approve all its personnel, substitutes or subcontractors. Changes to the named attendee shall be reviewed before access is granted, particularly where restricted research, production systems or confidential technical data are involved.

10.3 The access decision shall consider the actual work scope, completed induction, confidentiality obligations and any required competence. The organisation shall avoid collecting unrelated personal information or retaining document copies without a defined need. Adverse information shall be evaluated fairly, with appropriate review and correction channels rather than an automatic assumption of misconduct.

10.4 The approved record shall specify validity, sponsor, escort and permitted equipment. Reception shall check current status at arrival rather than rely on an old email or previous badge. Missing approval shall lead to a controlled waiting or rescheduling process, with urgent exceptions handled by an authorised role and fully recorded.

11 Visitor arrival and departure procedure

11.1 Before arrival, the sponsor shall register the visit, confirm the purpose and select a route that limits unnecessary exposure. Reception shall verify the visitor's identity and current authorisation, explain relevant safety and confidentiality rules and issue a time limited, visibly distinguishable credential. The visitor shall know whom to contact if separated from the host or an emergency occurs.

11.2 The host shall meet the visitor and maintain the required escort. The visit shall remain within the approved purpose, zones and time. Unplanned requests to photograph equipment, inspect a prototype or meet another team shall require the relevant owner's approval before the activity occurs. Courtesy or seniority shall not create an automatic exception.

11.3 During the visit, the host shall protect unattended screens, documents, samples and conversations along the route. Required safety briefings and protective equipment shall be completed before entering operational areas. The host shall not place a visitor in a hazardous environment merely to avoid using a more visible public route.

11.4 At departure, Reception shall recover or deactivate the credential and record the end of the visit. The sponsor shall confirm return of loaned items and resolve any incident or unexpected access. Lost badges and unexplained departures shall be assessed promptly, while visitor records shall be retained only for their authorised security and operational purpose.

12 Sponsorship escort and hosted activities

12.1 A sponsor shall be an accountable employee authorised to justify the visit or engagement. The sponsor shall understand the sensitivity of the areas and information involved and arrange appropriate supervision. Sponsorship shall not be delegated informally to an employee who lacks authority or has not received the visitor's approved scope.

12.2 Escort requirements shall be based on zone and activity risk. Where continuous escort is required, the escort shall remain able to observe and guide the visitor without compromising their own safety duties. If the escort must leave, the visitor shall move to an approved waiting area or transfer to another authorised escort through a recorded handover.

12.3 Group visits shall have a manageable group size, defined route and sufficient hosts to prevent unintended separation. Demonstrations shall use cleared information and equipment states. The host shall check background displays, whiteboards, prototypes and conversations before the group arrives, and shall brief presenters on the boundaries of permitted technical discussion.

12.4 After a hosted activity, the sponsor shall record deviations, unanswered disclosure requests and any material provided. Repeated breaches or impractical escort arrangements shall trigger a process review. The objective is controlled access that supports legitimate collaboration, not an informal expectation that visitors will infer restrictions that were never communicated.

13 Contractor engagement and work authorisation

13.1 Purchasing and the business owner shall define the contractor's deliverables, locations, systems, personnel and permitted methods before work begins. Security and the relevant asset owners shall assess access needs and confidentiality risks. The engagement record shall distinguish permission to enter the site from permission to operate equipment, alter software or receive technical information.

13.2 The contractor shall receive applicable induction and work instructions, including incident reporting, device use, data handling and subcontracting restrictions. Competence and safe work authorisations shall be verified for the actual task. A security badge shall not be interpreted as an electrical, lifting, machine maintenance or production change permit.

13.3 The work owner shall supervise progress against the approved scope and review requests for additional access. Temporary digital permissions shall be limited to the necessary systems and duration. Contractors shall use attributable identities, and the organisation shall avoid shared accounts that prevent reconstruction of who performed a sensitive action.

13.4 At completion, the owner shall verify deliverables, restore equipment to the authorised state, close access and reconcile data and materials. Unresolved defects, retained copies and continuing support obligations shall be documented. Payment approval shall not be used as the sole evidence that technical access has been removed or confidential assets have been returned.

14 Work boundaries and change permits

14.1 Each contractor task in a controlled area shall have a defined work boundary covering physical location, equipment, data, time and permitted actions. The work owner shall identify interfaces with production, maintenance and safety permits. Security restrictions shall be integrated with those processes rather than creating a parallel instruction that conflicts with safe isolation or emergency response.

14.2 Changes to the task shall be assessed before execution. A request to inspect a neighbouring machine, copy a controller programme or connect diagnostic equipment shall be reviewed by the relevant owner even when the contractor considers it a convenient troubleshooting step. The record shall show why additional access is necessary and what limits apply.

14.3 The work permit shall identify the approved tools and devices, required supervision, rollback arrangements and evidence of completion. Changes affecting product quality or conformity shall follow the appropriate engineering process. Security approval shall not authorise an unvalidated machine programme or a modification to a released vehicle configuration.

14.4 The owner shall close the permit after verifying the actual work, access removal and restoration of the area. Unexpected observations, files copied and materials removed shall be reconciled. If the scope cannot be confirmed, the affected equipment or data access shall remain controlled until a competent review establishes its condition and the required corrective action.

15 Subcontractors and personnel substitution

15.1 A supplier shall disclose proposed subcontractors and personnel substitutions when they affect controlled access or confidential work. Purchasing shall ensure that the engagement terms provide a practical approval and notification process. The organisation shall not assume that a supplier's internal employment decision automatically authorises a new person to enter restricted areas or access engineering data.

15.2 The business owner shall review the substitute's role, competence, identity and need for access. Relevant confidentiality, security and safe work requirements shall flow to the actual performing party. Where multiple organisations share a task, the record shall identify who supervises the work and who remains accountable for information handling and incident reporting.

15.3 Access permissions shall be issued individually and shall not be transferred by lending badges, accounts or remote access tokens. A new technician shall complete the required induction and authorisation before using a predecessor's work location. Urgent maintenance needs shall follow the controlled exception process rather than an informal handover of credentials.

15.4 The owner shall periodically reconcile active access against the current contractor roster and scope. Departed or reassigned personnel shall be removed promptly under the defined process. Discovery of undisclosed subcontracting shall trigger a factual assessment of work performed, information accessed and potential exposure, with proportionate containment and contractual action through authorised functions.

16 Onboarding transfer and offboarding

16.1 Human Resources, Purchasing and access administrators shall coordinate identity lifecycle events for employees and third parties. Onboarding shall establish the role, sponsor, required training and minimum permissions before access is activated. Role changes shall trigger review of existing rights so that permissions do not accumulate indefinitely across projects or departments.

16.2 The manager shall notify planned departures and engagement endings through the controlled process. The offboarding plan shall identify physical credentials, keys, devices, repositories, cloud shares, remote access, service accounts and confidential materials associated with the person. Ownership of ongoing work shall transfer to a named custodian before records become inaccessible.

16.3 Access removal shall follow the assessed risk and authorised timing, with verification across connected systems rather than reliance on one directory change. Shared secrets exposed to the departing person shall be reviewed for rotation where necessary, while preserving operational continuity. Personal information and employment actions shall be handled through the appropriate authorised functions.

16.4 Closure shall reconcile returned assets, remaining obligations, external copies and exceptions. The organisation shall retain evidence of completed removal and investigate unexplained access after departure. Offboarding shall not erase records needed for product safety, legal holds or investigations, and shall not be used to obstruct protected reporting or lawful access to personal employment information.

17 Badges keys and access reviews

17.1 The access administrator shall issue credentials to identified individuals for an approved purpose, zone and duration. Credentials shall be protected against sharing and shall display only the information needed for their use. Physical keys and master access devices shall have an inventory, authorised holders and a controlled issue and return record.

17.2 Lost, stolen or malfunctioning credentials shall be reported promptly and assessed for deactivation, replacement and possible exposure. A replacement shall not leave the old credential active without an approved reason. Security shall provide a practical reporting route so that staff do not postpone notification because the process is difficult or punitive.

17.3 Periodic access reviews shall compare permissions with current employment, contractor scope and business need. Asset owners shall confirm restricted rights individually or through a justified role mapping. A review completed by approving an unchanged list without checking its basis shall not be accepted as evidence that access remains appropriate.

17.4 Exceptions shall identify the reason, duration, compensating control and approving authority. The review shall include dormant credentials, unusual out of hours access and emergency permissions that have not expired. Metrics shall distinguish justified exceptional access from control failures, and findings shall lead to correction of the underlying provisioning or notification process.

18 Restricted research and development areas

18.1 The research owner shall define access conditions for laboratories, design studios, pilot workshops and other areas containing unreleased technology. Permissions shall reflect project need and the sensitivity of current work. General employment or access to the wider factory shall not automatically grant entry to restricted research areas.

18.2 The area owner shall control observation through doors, windows, screens and shared spaces. Sensitive prototypes and information shall be covered, stored or otherwise protected when unrelated personnel must enter. Cleaning, maintenance and emergency arrangements shall be planned so that essential services can occur safely with suitable supervision and limited exposure.

18.3 Project teams shall use approved repositories, controlled sample storage and attributable access. Shared workbenches, printers and meeting areas shall have clear rules for unattended material. The owner shall assess whether a visitor can infer sensitive information from labels, component combinations, test schedules or conversations even when no formal drawing is provided.

18.4 At project transition or closure, the team shall reconcile prototypes, data, equipment and external copies. Information needed for safety and product support shall remain available to authorised roles. Protection decisions shall be reviewed as the technology becomes public, avoiding permanent restrictions that no longer serve a legitimate purpose while preserving still confidential manufacturing knowledge.

19 Production cells and process knowledge

19.1 The production owner shall identify sensitive process information, including joining sequences, tool paths, recipes, fixtures, cycle optimisation and quality algorithms. The assessment shall distinguish ordinary operational visibility from information that requires restricted disclosure. Controls shall support production and maintenance without exposing complete process knowledge to every person who needs limited access to a machine.

19.2 Visitor and contractor routes shall limit unnecessary observation of restricted operations. Where equipment must be serviced, the owner shall provide the information needed for the task through an approved scope. A service technician's need to diagnose a fault shall not automatically justify copying the entire plant programme library or photographing unrelated stations.

19.3 Machine interfaces, printouts and local backups shall receive appropriate protection. Production personnel shall know how to handle requests for screenshots, programme exports or detailed performance data. The process owner shall authorise legitimate sharing and retain a record of what was provided, rather than requiring staff to make inconsistent informal decisions during a breakdown.

19.4 Changes to protection controls shall be checked for effects on safety, recovery and quality. Locking access to a machine shall not prevent authorised emergency action or timely restoration from a verified backup. The organisation shall test that necessary technical knowledge remains available to competent personnel while unauthorised copying and modification are appropriately restricted.

20 Prototypes models and unreleased vehicles

20.1 The programme owner shall assign unique identities to prototypes, mule vehicles, clay models and unreleased assemblies. The custody record shall identify configuration, location, responsible person, permitted use and disclosure restrictions. A prototype shall not become untracked because it is incomplete, nonfunctional or scheduled for destruction.

20.2 Storage, movement and demonstration plans shall address observation, photography, transport exposure and unauthorised access to onboard data. Protective coverings and concealment measures shall be assessed for safe handling, ventilation, visibility and operation. The team shall not modify safety critical systems or obstruct a driver's view merely to improve visual secrecy.

20.3 Road or external testing shall use the required legal permissions, competent personnel and an approved operational plan. The security plan shall coordinate with test safety and incident response. Any loss, collision, unauthorised observation or unexpected custody change shall be reported factually, preserving technical and safety evidence before making assumptions about deliberate interference.

20.4 After use, the owner shall reconcile parts, data, keys and test equipment and decide retention, conversion or disposal. Disposal shall prevent unintended release of confidential design features while meeting environmental and record obligations. A public launch shall trigger review of classification, but shall not automatically make all prototype data or manufacturing knowledge public.

21 Tooling additive files and controlled scrap

21.1 Tooling owners shall inventory dies, moulds, fixtures, gauges and additive manufacturing files that embody sensitive geometry or process knowledge. The record shall identify ownership, location, permitted users, maintenance rights and return conditions. Tooling located at a supplier shall remain within the organisation's custody and contract oversight arrangements.

21.2 Transfers for repair, duplication or production relocation shall require an authorised work scope and chain of custody. The receiving organisation shall receive only the information needed for the task. Requests to retain geometry, create additional copies or use the tooling for another customer shall be assessed by the asset owner and Legal function before permission is granted.

21.3 Scrap, rejected parts, printed prototypes and obsolete tooling shall be classified before leaving controlled custody. The disposition method shall address both environmental requirements and disclosure risk. Destruction shall be appropriate to the asset and performed safely by an authorised provider; the manual does not prescribe hazardous destruction methods or assume that visual damage makes technical information unrecoverable.

21.4 The owner shall reconcile quantities or unique identities and retain evidence of return, destruction or approved reuse. Disposal records shall not replace necessary product quality, traceability or legal hold records. Exceptions, missing items and unexplained differences shall be investigated through a proportionate process with clear responsibility for closure.

22 Photography recording and personal devices

22.1 The site shall define where photography, video, audio recording and personal devices are permitted, restricted or prohibited for a justified purpose. Rules shall be communicated before entry and applied consistently. Restrictions shall account for emergency communication, accessibility needs and lawful reporting, rather than imposing an unexplained blanket ban that staff cannot implement safely.

22.2 Authorised recording shall have an owner, subject, purpose, permitted area and approved device or channel. Before capture, the owner shall check backgrounds, screens, labels, people and adjacent prototypes for unintended disclosure. Images intended for external use shall receive a release review that considers technical confidentiality, personal data and third party rights.

22.3 Devices used by visitors and contractors shall be managed through the agreed access process. Where secure storage or device restrictions are required, the arrangement shall be proportionate and practical. Security staff shall not conduct unauthorised searches of personal content or compel access outside their lawful powers and approved procedure.

22.4 Approved recordings shall be stored, shared and retained under the assigned classification. Unauthorised recording concerns shall be reported and assessed without unsafe confrontation. The response shall preserve relevant evidence and involve authorised Legal, Privacy or Human Resources roles as needed, distinguishing accidental capture from deliberate misconduct and recording the basis for any corrective action.

23 Meetings displays and technical demonstrations

23.1 Meeting organisers shall assess attendees, subject matter and information classification before selecting a room or online platform. The invitation shall identify participation limits and any recording conditions. External attendees shall receive only the materials approved for their purpose, with access configured to prevent unnecessary onward sharing where practicable.

23.2 Presenters shall review slides, live systems, browser tabs and demonstration data for unrelated confidential content. Screen sharing shall use the minimum necessary window or application. Demonstrations should use prepared datasets or controlled environments when live production or customer information would create avoidable exposure, while clearly identifying any simulated information.

23.3 Rooms and shared areas shall be checked before and after meetings for whiteboards, printouts, models and unattended devices. Remote participants shall be verified through the approved process for sensitive sessions. A familiar display name or forwarded invitation shall not establish identity or permission to attend a restricted technical discussion.

23.4 The organiser shall retain the approved material and record significant disclosures, recording permissions and follow up requests. Minutes shall separate decisions from sensitive technical detail where appropriate without losing accountability. External publication, exhibition or customer demonstration shall receive a specific release review rather than relying on approval of an earlier internal meeting.

24 Deliveries drivers and loading areas

24.1 Logistics shall define arrival instructions, identity checks, vehicle routes, waiting areas and loading responsibilities for carriers and delivery personnel. Access shall be limited to the approved task and locations. A delivery appointment shall not authorise the driver to enter research areas, inspect production or use internal digital systems.

24.2 Loading areas shall be arranged to reduce exposure of unrelated goods, labels and confidential prototypes. The responsible employee shall verify shipment identity and authorisation before goods are released. Unexpected collection requests, changed vehicles or substitute drivers shall be checked through a trusted contact route rather than accepted solely from documents presented at the gate.

24.3 Inspection and seal controls shall be matched to the cargo risk and performed safely. Security staff shall follow lawful search and inspection procedures and shall not assume authority to detain people or seize personal property. Suspected theft, tampering or unlawful activity shall be escalated to the appropriate authorised function or public agency.

24.4 Records shall link goods, carrier, driver verification, loading time, seal or custody information and exceptions. Discrepancies shall trigger a hold on the affected shipment while the responsible owner confirms the facts. Operational delays shall be managed through Logistics so that pressure to clear a queue does not bypass the release and custody checks.

25 Secure transport and offsite custody

25.1 The asset owner and Logistics shall assess transport risks for prototypes, sensitive tooling, samples and engineering media. The plan shall identify the permitted route, carrier capability, packaging, custody handovers and communication arrangements. Detailed routes and tracking access shall be restricted to roles that need them for safe and reliable execution.

25.2 Carrier agreements shall define subcontracting, unattended storage, incident notification and proof of delivery requirements. The team shall assess intermediate depots and cross border handling where custody or observation risks change. A premium transport service shall not be assumed secure without verifying the actual arrangements used for the consignment.

25.3 Tracking shall support proportionate cargo protection and operational response, with personal data implications assessed where individuals can be identified. Loss of tracking, route deviation or an unexpected handover shall trigger verification through approved channels. The response shall avoid directing unsafe driving, confrontation or unauthorised recovery activity merely to protect an asset.

25.4 On receipt, the custodian shall verify identity, condition, seals where used and completeness against the dispatch record. Damage, tampering or missing items shall be documented before routine use. The owner shall decide whether technical inspection, data integrity checks or security investigation are required and shall preserve evidence without disrupting necessary emergency action.

26 Samples loans and external technical work

26.1 Every external loan of a sample, prototype, drawing set or test article shall have an identified owner, recipient and permitted purpose. The agreement shall define allowed analysis, copying, subcontracting, publication, retention and return or destruction. The scope shall be specific enough to distinguish authorised testing from unrelated technical extraction.

26.2 The release package shall contain only the information and physical features needed for the task where practical. The owner shall assess whether labels, embedded storage, diagnostic interfaces or attached files expose additional confidential information. Sanitisation shall preserve the validity and safety of the authorised work; it shall not alter a test article in a way that makes the resulting evidence misleading.

26.3 Custody records shall follow the item through shipment, receipt, use and return. The recipient shall report loss, unauthorised access, unexpected subcontracting and material changes. The organisation shall agree in advance how test data, destructive remnants and derived results will be handled, including rights needed for safety or compliance evidence.

26.4 At closure, the owner shall reconcile items and information, verify agreed return or deletion and record any permitted residual copies. A certificate of destruction shall be evaluated against the provider and method rather than accepted as absolute proof. Unresolved discrepancies shall remain open with proportionate containment and an authorised decision on further action.

27 Digital identities and least privilege

27.1 Information Security shall provide attributable identities and access limited to the approved role, project and purpose. Sensitive engineering and administrative access shall use authentication appropriate to the risk, with additional verification for privileged or remote activity. Shared accounts shall be avoided, and necessary technical exceptions shall have ownership, traceability and a compensating control.

27.2 Permissions shall distinguish viewing, editing, exporting, administration and external sharing. Access to a repository shall not automatically grant permission to download complete programmes or invite outside collaborators. The asset owner shall approve the access scope, while administrators shall implement and verify it without expanding the business decision for convenience.

27.3 Joiner, mover and leaver events shall reach all relevant systems, including cloud platforms, supplier portals and local engineering tools. Privileged access shall be time limited where practical and reviewed against actual use. Service accounts and machine identities shall have owners, defined purposes and protected credentials rather than being treated as permanently exempt from review.

27.4 The organisation shall monitor failed provisioning, dormant access and unexplained privilege changes through a proportionate process. Access reviews shall test a sample of actual system rights against approved requests. When a mismatch is found, the team shall correct the permission and examine whether other users or systems are affected by the same provisioning rule.

28 Engineering repositories and version integrity

28.1 Engineering repositories shall store controlled drawings, models, code, specifications and change records with version history and attributable actions. The system shall distinguish working branches, reviewed baselines and released production data. Permissions shall protect both confidentiality and integrity so that an unauthorised modification cannot quietly become an approved manufacturing instruction.

28.2 The asset owner shall define export and sharing controls based on project need and information sensitivity. Bulk downloads, replication and integration with other platforms shall receive specific assessment. Technical controls shall be tested for their actual effect, including cached copies and synchronised folders, rather than assuming that a visible access setting controls every downstream copy.

28.3 Backups shall preserve recoverable versions and be protected from the same compromise that could affect the primary repository. Restore tests shall verify usable content, permissions and configuration integrity. Backup access shall be restricted, since a complete backup may expose more information than ordinary project permissions allow.

28.4 Change records shall link approvals to the exact content released. Suspected unauthorised edits shall trigger containment and comparison against a verified baseline before production use resumes. The organisation shall preserve the history needed for product quality and investigations, avoiding ad hoc deletion that destroys evidence of who changed a design or when an affected file was used.

29 External collaboration and technical data sharing

29.1 The business owner shall define the collaboration purpose, participants, required information and expected outputs before opening an external workspace. Legal and asset owners shall establish rights to use, modify, retain and publish both input and resulting information. A general cooperation agreement shall not automatically permit access to every project or another party's confidential data.

29.2 The sharing process shall minimise the package to the task, verify recipients and use an approved channel. Access shall have an expiry or review event and shall distinguish download, edit and onward sharing permissions. The owner shall assess whether derived files, metadata and embedded history reveal additional information beyond the visible drawing or model.

29.3 Sensitive releases shall receive an independent check of recipient, package and authority before transmission. The sender shall retain the released version and a record of the purpose and conditions. Requests for expanded access shall return to the owner rather than being fulfilled through an informal link or a copied folder from another project.

29.4 At collaboration closure, the team shall reconcile deliverables, retained rights and external copies. Continuing access shall have a defined reason and owner. Security concerns shall be handled through the agreed incident process, while legitimate safety disclosures, required evidence access and lawful contractual rights shall remain available under controlled arrangements.

30 Remote support and operational technology access

30.1 Remote access to production or engineering systems shall require an approved purpose, named user, defined target and limited duration. The system owner shall coordinate with Operations, Information Security and the contractor sponsor. An urgent breakdown shall trigger the emergency access procedure rather than an unmanaged connection that remains open after the repair.

30.2 The access design shall use approved secure gateways and authentication, with permissions limited to the required systems and functions. Sessions shall be supervised or recorded where proportionate and lawful for the risk. Remote users shall not receive broad plant network access merely because a diagnostic tool is easier to operate that way.

30.3 Before changes, the owner shall confirm backups, safe operating conditions, authorised work scope and recovery arrangements. Actions affecting machine safety, quality or product configuration shall follow their respective change procedures. Security approval alone shall not authorise a control logic change or the bypass of a protective function.

30.4 At completion, the owner shall review the work, verify system state, remove temporary access and retain relevant session and change evidence. Unexpected activity shall trigger containment under the incident process. The IAF Connected Factory and OT Cybersecurity Manual, IAF-MAN-OTC-001, shall govern detailed technical controls, with this manual retaining responsibility for third party purpose and access boundaries.

31 Removable media and portable equipment

31.1 The organisation shall define which removable media and portable devices may connect to engineering and production systems. Approved media shall have an owner, identity, intended use and handling rules. Unverified devices shall not be connected merely to discover their contents, and personal storage shall not be used as a shortcut around controlled transfer processes.

31.2 Transfers shall use a controlled intake or verification process appropriate to the environment, including checks for malicious content and configuration integrity. The process shall account for systems that cannot safely run ordinary scanning tools or tolerate unplanned interruption. Technical personnel shall select validated methods rather than apply a universal procedure that could disrupt production equipment.

31.3 Portable service equipment shall be configured and maintained for its authorised purpose, with unnecessary access and stored data minimised. The sponsor shall verify what information may be copied from the site and where it may be retained. A contractor's diagnostic laptop shall not become an uncontrolled archive of multiple customers' machine programmes.

31.4 Media loss, unexpected files or suspected compromise shall be reported promptly and handled as evidence where relevant. Sanitisation and disposal shall use an approved method suited to the medium and sensitivity, with verification recorded. Required production and safety records shall be transferred to controlled storage before devices are erased or returned.

32 Machine programmes and production backups

32.1 Machine programmes, robot paths, process recipes and associated configuration files shall have identified owners and controlled release states. The organisation shall distinguish information needed for routine operation from information requiring restricted engineering access. Local copies shall be reconciled with the authorised baseline so that maintenance convenience does not create an untracked alternative source of production instructions.

32.2 Backups shall include the data and dependencies needed for safe restoration, with version, equipment identity and creation date. They shall be protected against unauthorised copying and alteration. A backup shall be considered usable only after a suitable restore or verification exercise demonstrates that the required content can be recovered and interpreted by competent personnel.

32.3 Programme exports to suppliers or service providers shall follow the technical sharing process. The owner shall assess whether a reduced diagnostic package can satisfy the task without releasing the complete process library. Restrictions shall still allow necessary safety analysis, recovery and contracted service, with any limitations agreed before an urgent failure occurs.

32.4 Changes shall be attributable and approved through engineering and operational controls. After remote or onsite support, the owner shall verify the actual programme against the authorised change and retain evidence of the final state. Unexpected differences shall trigger a quality and security assessment before the affected equipment returns to unrestricted production.

33 Cloud platforms artificial intelligence and digital twins

33.1 The asset owner shall approve the use of cloud platforms, artificial intelligence tools and collaborative digital twin environments for engineering information. The assessment shall identify data locations, access rights, service providers, permitted processing and contractual use of submitted content. A convenient interface or existing corporate subscription shall not automatically authorise restricted technical data in every feature of the service.

33.2 Before uploading, the user shall verify the purpose, information classification and allowed dataset. The organisation shall assess prompts, attachments, model outputs, logs and integrations, since each may expose confidential geometry, code or process knowledge. Where a reduced or synthetic dataset is used, its limitations shall be clear so that the resulting engineering conclusions are not overstated.

33.3 Digital twin access shall distinguish visual observation, simulation, model export and control connections to physical equipment. External participants shall receive only the functions required for the collaboration. A virtual factory can reveal sensitive layouts, cycle logic and asset relationships, and shall therefore be assessed as an engineering asset rather than treated as a harmless visual presentation.

33.4 Outputs shall undergo technical and confidentiality review before production use or external release. The owner shall manage retention, deletion, account closure and provider changes, including residual data in logs or backups where relevant. Unapproved disclosure to a service shall enter the incident process, with truthful assessment of what was shared and what recovery is actually possible.

34 Data loss monitoring and alert handling

34.1 Information Security shall define monitoring aimed at detecting unauthorised technical data transfer, account misuse and unusual access. The design shall state the purpose, data collected, access to results, retention and review authority. Monitoring shall be proportionate and lawful, with appropriate notice and consultation rather than hidden collection justified by a vague security objective.

34.2 Alerts shall be assessed in context, considering approved bulk work, backups, collaboration and role changes. A large download or unusual working hour is an indicator for review, not proof of theft. Analysts shall document the facts and seek authorised business context before escalating to an allegation or employment action.

34.3 The response procedure shall define who can restrict a share, revoke a token or isolate an endpoint and how operational consequences are assessed. Actions affecting production shall be coordinated with the system owner and safe operating requirements. The team shall preserve relevant logs and file identity without unnecessarily copying unrelated personal content.

34.4 Monitoring effectiveness shall be reviewed through authorised tests and incident outcomes. Excessive false positives, missed events and unclear ownership shall lead to tuning and process correction. The organisation shall not use security telemetry for unrelated employee evaluation without a separate lawful basis and transparent governance, and shall restrict investigative access to those with an approved need.

35 Cameras biometrics and privacy safeguards

35.1 The site shall assess camera and biometric controls individually for a defined protective purpose. The assessment shall consider less intrusive alternatives, affected people, field of view, data sensitivity and legal requirements. Biometric processing shall not be introduced merely because a device supports it or because it appears more modern than a conventional credential.

35.2 Camera placement shall avoid unnecessary capture of private areas and unrelated neighbouring activity. Access to recordings shall be role based and logged, with a defined retention schedule and secure export process. Signs and notices shall communicate the relevant monitoring information in a form people can understand before entering the monitored area where required.

35.3 Requests to retrieve footage shall identify the incident, time window, purpose and approving role. Exported evidence shall preserve integrity and custody while limiting unrelated personal data. Routine retention shall be suspended for a relevant legal or investigation hold, and the hold shall be reviewed rather than becoming an indefinite reason to keep all recordings.

35.4 The organisation shall test equipment condition, time accuracy and actual coverage without publishing sensitive blind spots. Monitoring shall not replace physical response, safe work controls or fair investigation. Intrusive or covert measures shall not be initiated by local staff outside the lawful authority and formal approval process established with Legal, Privacy and Human Resources.

36 Insider concerns and protected reporting

36.1 Employees and contractors shall have accessible channels to report suspected unauthorised disclosure, access misuse, coercion or other security concerns. Reports shall be received respectfully and assessed on evidence. The organisation shall explain confidentiality limits honestly and shall not promise anonymity that the reporting system or investigation process cannot actually provide.

36.2 Security and Human Resources shall distinguish deliberate misconduct, error, poor process design and legitimate activity. Indicators shall be evaluated in context and without discriminatory profiling. A person raising a safety, labour, privacy or compliance concern shall not be treated as an insider threat merely because the report is inconvenient or critical of management.

36.3 The IAF Whistleblowing Policy shall govern protected reporting and anti retaliation arrangements. Access restrictions needed to preserve an investigation shall be proportionate and shall not become a disguised punishment before findings are established. Conflicts involving senior staff or the usual investigator shall be escalated to an independent authorised reviewer.

36.4 Case records shall limit access, preserve evidence and track actions and outcomes. The organisation shall inform relevant parties through the appropriate process while respecting privacy and investigation needs. Lessons shall address systemic weaknesses and reporting barriers, not only individual conduct, and management shall review whether staff can raise concerns without fear of improper consequences.

37 Contracts intellectual property and confidentiality

37.1 The business owner and Legal function shall define rights and obligations before confidential technical work begins. Agreements shall identify the information, permitted purpose, authorised recipients, security expectations, incident notice, return or deletion and treatment of derived results. Generic confidentiality language shall be supplemented by an operational sharing and access plan.

37.2 Ownership of background knowledge, newly developed results, tooling, software and test data shall be addressed explicitly. The organisation shall verify that it has the right to share third party information and that necessary rights for product safety, compliance, maintenance and continuity are preserved. A supplier relationship shall not be assumed to transfer all intellectual property automatically.

37.3 Restrictions shall be reviewed for enforceability and compatibility with applicable law, including competition, labour, privacy and legitimate disclosure rights. Contractual terms shall not be described as binding on the entire automotive sector or on parties that have not accepted them. IAF participation shall not create ownership of another organisation's technology.

37.4 Contract management shall verify implementation through approved recipients, controlled repositories, incident contacts and closure records. Disputes shall be handled through the agreed lawful process. Security personnel shall preserve evidence and support counsel, but shall not threaten penalties, seize assets or compel disclosure beyond the organisation's actual contractual and legal authority.

38 Reverse engineering protection and lawful boundaries

38.1 The asset owner shall identify which technical knowledge is protected by confidentiality, intellectual property rights, access restrictions or a combination of measures. Protection strategy shall distinguish information kept secret from features observable in products lawfully available to the public. The organisation shall obtain a jurisdiction specific assessment before asserting that another party's analysis is prohibited.

38.2 Unauthorised acquisition from restricted systems, breach of a valid confidentiality obligation and misuse of entrusted prototypes shall be addressed through evidence based controls and lawful remedies. Independent development, observation or reverse engineering may be lawful depending on the circumstances. The manual shall not be used to claim a universal monopoly over automotive methods or to suppress legitimate competition.

38.3 Engineering shall select proportionate measures such as controlled disclosure, compartmentalised access, secure development interfaces and traceable sample loans. The measures shall preserve product safety, required inspection, repair and customer rights. A trade secret label shall be supported by actual protective practices and shall not replace a reasoned decision about what information can remain confidential after market release.

38.4 Suspected infringement or misappropriation shall be assessed with Legal using the actual rights, access history and evidence. Public accusations shall not be made solely from product similarity. The response shall distinguish a substantiated breach from a technical resemblance that may have an independent explanation, with corrective action directed to the proven facts and legitimate interests at risk.

39 Product tamper controls and service access

39.1 Product engineering shall assess protective controls for development interfaces, diagnostic access, software authenticity and physical tampering according to the product risk. The design shall define authorised manufacturing, service, recovery and investigation functions. Security measures shall be reviewed with safety and service teams so that protection does not create an unsafe failure mode or prevent necessary repair.

39.2 Development capabilities shall be removed, restricted or governed appropriately before production release. The organisation shall verify the actual state of shipped products and retain evidence of configuration. A written instruction to disable an interface shall not establish that every vehicle or component was configured correctly.

39.3 Authorised service access shall use controlled identities, tools and procedures appropriate to the task. Rights required by law or contract shall be implemented through workable arrangements. Protection of technical information shall not be used to deny safety related service information, obstruct a lawful inspection or conceal a product defect.

39.4 Anti tamper features shall not include destructive retaliation or unsafe self disabling behaviour in response to suspected analysis. Changes to access controls shall be assessed for recovery, emergency use and product conformity. Field incidents involving tampering shall be evaluated factually, recognising that damage, software faults and legitimate repair can sometimes produce indicators that resemble deliberate interference.

40 Competitive benchmarking and clean separation

40.1 The organisation shall govern its own competitive analysis with the same respect for rights expected from others. The project owner shall document the lawful source of products and information, permitted activities and any contractual restrictions. Staff shall not solicit confidential material from a competitor's employee or use unauthorised access as a shortcut to engineering knowledge.

40.2 Benchmarking instructions shall distinguish publicly available information, licensed data, purchased products and confidential material received under restriction. Legal shall assess uncertain rights before analysis proceeds. The team shall preserve provenance and avoid mixing questionable information into design repositories where its origin may later become impossible to separate.

40.3 Where a clean separation process is appropriate, roles, information boundaries and review steps shall be defined before work begins. The process shall create a verifiable record of independent requirements and development inputs; a label such as clean room shall not be treated as automatic legal protection. The actual method and jurisdiction determine its significance.

40.4 Results shall undergo review before reuse, publication or patent related decisions. Unexpected receipt of another party's confidential information shall trigger containment and authorised advice rather than circulation within the project. The organisation shall correct improper acquisition or use and retain evidence of its response without making unsupported claims that all competitive learning is forbidden.

41 Incident intake and initial triage procedure

41.1 The receiver shall record the reported event, time, location, affected assets and immediate safety concerns. The record shall preserve the reporter's account without converting assumptions into findings. If there is danger to people or an active emergency, the site emergency process takes priority and public emergency services shall be contacted through the approved route.

41.2 Security shall verify enough information to classify the event and identify the appropriate response lead. The assessment shall consider ongoing access, possible data exposure, production interference, personal data and evidence at risk. Severity shall reflect potential impact and uncertainty; a low volume disclosure may be significant if it contains a critical design or credential.

41.3 The incident lead shall notify the necessary asset, information security, legal, privacy, human resources and operational roles. Access to the case shall be limited to those needed for response. The team shall establish a secure communication channel and record decisions, avoiding broad internal messages that disclose sensitive details or make premature accusations.

41.4 Initial actions shall be proportionate and reversible where possible, such as restricting an exposed share or preserving relevant logs. The lead shall define the next evidence needed, action owners and review time. The incident remains open until its scope and required response are established; absence of an immediate visible loss shall not be treated as proof that no exposure occurred.

42 Containment and evidence preservation procedure

42.1 The incident lead shall select containment based on the affected asset, ongoing risk and operational consequences. Digital actions may include revoking a specific token, restricting a repository or isolating an affected device through authorised technical procedures. Physical actions may include securing a room or pausing a shipment. Production and life safety effects shall be assessed before intervention.

42.2 Evidence shall be preserved by competent personnel using methods appropriate to the source. The record shall identify what was collected, by whom, when, from where and how integrity was protected. Original data shall remain available where feasible, with working copies used for analysis and cryptographic integrity checks applied where suitable.

42.3 Collection shall be limited to the authorised scope and shall respect privacy, employment and legal requirements. Security staff shall not conduct uncontrolled searches of personal devices, secretly intercept communications or seize property beyond their authority. Where public authorities are needed, the organisation shall coordinate through authorised Legal and Security contacts.

42.4 The lead shall maintain a custody log and record any action that changes evidence, including necessary emergency shutdown or account removal. Preservation shall not delay rescue or create an unsafe condition. Legal holds shall identify the relevant records and custodians, and shall be reviewed and released through an authorised decision when the preservation obligation ends.

43 Investigation fairness and disclosure decisions

43.1 The investigation sponsor shall define the scope, investigator competence, independence and decision authority. The plan shall identify the questions to be answered, evidence sources and legal limits. Where the concern involves senior management or the normal response team, an independent authorised investigator shall be appointed to avoid a conflict that undermines the findings.

43.2 Investigators shall test alternative explanations and distinguish technical indicators from proof of intent. Interviews shall follow the applicable employment and legal process, with accurate records and appropriate support. The organisation shall not use threats, discriminatory assumptions or unsupported public allegations to obtain a convenient admission.

43.3 Legal and Privacy shall assess required notifications to affected parties, authorities, partners or insurers using the actual facts and applicable obligations. Verified deadlines and decision reasons shall be recorded in the case. Confidentiality shall support a sound investigation but shall not suppress mandatory disclosures, product safety reporting or protected whistleblowing.

43.4 The final finding shall state what is established, what remains uncertain, the affected assets and the basis for corrective action. Employment, contractual and legal outcomes shall be decided by the authorised functions. Case closure shall include access restrictions, record retention and communication responsibilities, with a route to correct material factual errors through the applicable process.

44 Recovery and controlled restoration procedure

44.1 The recovery owner shall define the conditions for restoring access, systems, equipment or an external engagement after an incident. Conditions shall address the cause of exposure, integrity of affected assets, credential security and necessary quality or safety verification. A system becoming available again shall not be treated as proof that it is trustworthy or correctly configured.

44.2 Restoration shall use verified baselines and authorised technical procedures. Engineering and Operations shall confirm that recovered programmes, drawings and production settings match the approved state. Where an incident may have altered product configuration or manufacturing output, Quality and Homologation shall assess the affected population before normal release resumes.

44.3 Access shall be restored according to current need and role, avoiding automatic reinstatement of permissions that contributed to the incident. Temporary monitoring or additional review shall have a defined purpose, duration and owner. The organisation shall verify that legitimate users can complete essential work without relying on the same uncontrolled workaround that caused the original weakness.

44.4 Closure shall require evidence of effective corrective action, updated records and completion of required communications. Lessons shall address design, training, contracts and management decisions as well as technical controls. Remaining uncertainty shall be documented, and the accountable owner shall decide any permissible residual risk within legal, safety and contractual limits.

45 Emergency access and business continuity

45.1 The site shall predefine emergency access arrangements for rescue, urgent safety work and critical recovery. The process shall identify authorised decision makers, minimum verification, temporary permissions and logging. Emergency access shall be available when needed without becoming a permanent bypass for ordinary convenience or delayed planning.

45.2 During a power, network or identity service outage, Security and Operations shall activate the approved manual process. Entries shall record the person, purpose, sponsor, zone and time using a controlled temporary record. Restricted activities that cannot be safely or reliably supervised shall remain paused until a suitable control is restored.

45.3 Emergency responders shall receive necessary access and information for their lawful task. Confidentiality concerns shall not obstruct evacuation, rescue, hazard identification or required public authority action. Sensitive information provided during the event shall be documented when practical, but record completion shall not delay an urgent protective response.

45.4 After the emergency, the owner shall revoke temporary rights, reconcile manual logs and review actions performed. Any unverified changes or missing custody information shall enter the appropriate quality or security process. Coordination with IAF-MAN-BCP-001 shall ensure that continuity arrangements preserve essential access while maintaining traceability, technical integrity and a controlled return to normal operation.

46 Competence awareness and scenario exercises

46.1 The competence plan shall distinguish Security staff, sponsors, reception, asset owners, system administrators and ordinary users. Each role shall learn the decisions it must make and the limits of its authority. Practical assessment shall include identity discrepancies, unexpected disclosure requests, lost devices and safe incident escalation rather than relying only on annual attendance records.

46.2 Training shall use realistic automotive examples such as a service contractor requesting a programme export or a visitor photographing a prototype in the background. Staff shall practise how to pause the activity, contact the owner and preserve a factual record without confrontation. The organisation shall explain approved ways to obtain urgent legitimate access so that controls remain workable.

46.3 Exercises shall coordinate physical and digital response, including off hours conditions and absent key personnel. Participants shall retrieve actual procedures and demonstrate handovers, containment authority and evidence preservation. Simulated credentials and fictional data shall be used, and exercises shall not involve unauthorised intrusion or deceptive activity beyond the approved scope.

46.4 The exercise owner shall record strengths, gaps, responsible actions and effectiveness checks. Evaluation shall consider safety, fairness, privacy and decision quality alongside response time. Repeated errors shall trigger changes to system design or instructions rather than assuming that more reminders alone will correct an impractical or ambiguous process.

47 Audit metrics and management review

47.1 The audit programme shall test whether approved access and handling rules match actual practice. Samples shall include visitors, contractors, role changes, external shares, prototype loans and disposal records. Auditors shall trace both successful cases and exceptions, with sufficient independence from the control owner and protection for sensitive findings.

47.2 Metrics shall define their population, period and data source. Useful measures include overdue access removals, unowned restricted assets, unreconciled loans, expired exceptions and time to contain verified exposure. A high access review completion rate shall be accompanied by evidence of substantive checking; a signature on an unchanged list is not proof of effective review.

47.3 Management shall assess repeated weaknesses, resource gaps, incident trends and the practical burden of controls. Targets shall not reward underreporting or rapid case closure without evidence. The review shall assign actions and verify that corrective measures reduce the actual exposure rather than merely increase the number of forms completed.

47.4 Audit records shall distinguish a procedural gap from confirmed misconduct and shall avoid unnecessary personal detail. Corrective action shall address causes, affected scope and effectiveness. Significant unresolved risks shall reach the accountable director, with decisions recorded within lawful authority and without using risk acceptance to waive safety, privacy or other mandatory obligations.

48 IAF interfaces records and revision control

48.1 This manual operates with IAF-QM-001, the IAF Documents and Records Guide and the IAF policies for privacy, conflicts, complaints and protected reporting. Detailed operational technology controls connect to IAF-MAN-OTC-001; prototype work to IAF-MAN-NPI-001; continuity to IAF-MAN-BCP-001; and conformity related changes to IAF-MAN-HLC-001. Each interface shall identify the handover owner.

48.2 Security records shall be classified and retained according to purpose, legal requirements, contracts and investigation needs. The schedule shall distinguish routine visitor logs, access approvals, technical custody records and incident evidence. Retention shall have an event, period or review rule, custodian and disposal authority, with legal holds overriding routine deletion where applicable.

48.3 The document owner shall review this manual after significant incidents, new collaboration technologies, site changes and material legal developments. Revisions shall follow the competent IAF authority and document control process, with a change summary and communication to affected users. Sensitive site supplements shall be updated through controlled access without publishing operational vulnerabilities.

48.4 Adopting organisations shall verify implementation and competence before changed controls take effect. IAF membership, Corporate Recognised status and committee participation shall follow the relevant federation guides and shall not create powers to compel third parties or restrict lawful competition. The operating organisation remains responsible for proportionate protection, safe operations, truthful claims and lawful treatment of people and information.

Annex A Adoption asset and zone register

Complete an adoption record for each site and maintain linked asset and zone registers. Keep sensitive locations and protection details in the controlled operating record.

Record field	Required entry and evidence
Operating identity	Record legal entity, site, manual code and revision, actual adoption date and accountable director.
Asset ownership	List asset identifiers, owners, custodians, sensitivity, permitted uses and lifecycle stage.
Zone definition	Record zone owner, boundaries, entry conditions, escort rules and permitted activities.
Legal and safety review	Link assessments of privacy, monitoring, employment, emergency egress and required consultation.
Control implementation	Identify access systems, local procedures, training and evidence that the controls operate.
External custody	List suppliers, laboratories, carriers and platforms holding assets, with scope and return obligations.
Gaps and exceptions	Record missing controls, interim measures, decision authority, expiry and closure evidence.
Review triggers	Include layout changes, new programmes, incidents, technology changes and revised obligations.

Public copies shall not include detailed security maps, credentials or operational vulnerabilities. Publication does not itself demonstrate site readiness.

Annex B Individual access request and review

Use one request for a named individual and defined purpose. Approval to enter a facility shall not automatically authorise equipment operation or digital access.

Record field	Required entry and evidence
Person and sponsor	Enter identity, employer, role, sponsor and verified business contact using only necessary personal data.
Purpose and scope	State the task, deliverable, required zones, systems and information classification.
Validity	Record start, end, working hours and the event that requires review or immediate removal.
Prerequisites	Confirm identity verification, induction, confidentiality, competence and safe work authorisations as applicable.
Permission detail	Specify view, edit, export, remote support, escort and device conditions separately.
Approvals	Record asset owner, Security, system owner and other required decisions with actual dates.
Implementation check	Verify that issued badges and system rights match the approved scope; record administrator and evidence.
Review and closure	Confirm continuing need, changed role, revoked rights, returned credentials and unresolved exceptions.

Do not transfer badges or accounts between people. A review shall compare actual rights with current need rather than simply renew a previous approval.

Annex C Visitor visit and escort record

Create before arrival and complete at departure. The sponsor remains responsible for the approved purpose and information exposure during the visit.

Record field	Required entry and evidence
Visit identity	Enter visitor, organisation, sponsor, purpose, date and approved meeting or activity.
Entry verification	Record verified authorisation and identity check outcome without unnecessary document copying.
Route and zones	Identify approved areas, waiting location, escort and any required handover.
Briefing	Confirm safety instructions, emergency information, confidentiality and recording or device rules.
Credential	Record badge identifier, validity, issue and return or deactivation.
Activity changes	Log requests for additional areas, photographs, samples or technical information and the owner's decision.
Departure reconciliation	Confirm end time, returned items, loan closure and any unexpected access or incident.
Retention	Assign record custodian, lawful purpose, access controls and retention or hold rule.

Use a separate incident record for material concerns. Visitor logs shall remain factual and shall not contain unsupported allegations or unrelated personal observations.

Annex D Contractor work scope and closure

Use with the applicable safety and engineering work permits. Security approval defines access boundaries and does not replace technical or safe work authorisation.

Record field	Required entry and evidence
Engagement	Record supplier, named personnel, approved subcontractors, business owner and contracted deliverable.
Work boundary	Specify locations, equipment, systems, information, duration and permitted actions.
Tools and devices	List approved diagnostic equipment, removable media, remote connections and data transfer methods.
Prerequisites	Link induction, competence, confidentiality, safety permits, backups and recovery arrangements.
Change requests	Record additional access or task changes, justification and approvals before execution.
Work evidence	Retain actions performed, files exported, programme changes, materials removed and supervision records.
Technical closure	Verify equipment state, quality and safety checks, approved configuration and remaining defects.
Access closure	Remove temporary rights, recover credentials, reconcile retained data and confirm continuing support obligations.

An invoice or completed purchase order is not evidence that access has been closed. Reconcile the actual work and the information handled.

Annex E Device photography and publication permission

Complete before recording or releasing technical imagery. Review the entire capture, including background information and personal data.

Record field	Required entry and evidence
Request	State requester, purpose, intended audience, location and proposed recording date.
Subject	Identify equipment, prototype, drawing, demonstration or people to be recorded.
Device and channel	Specify approved device, storage, transfer method and any contractor equipment conditions.
Exposure review	Check screens, labels, geometry, adjacent work, conversations, metadata and third party information.
Permission limits	Define allowed views, recording type, duration, recipients and whether onward publication is permitted.
Authorisation	Record asset owner and required Privacy, communications or contractual approvals.
Final release	Link reviewed files and versions, actual recipients and any editing or redaction performed.
Closure	Record retention, deletion of unused captures, incident handling and continuing use restrictions.

Permission to take an image and permission to publish it are separate decisions. Security staff shall not search personal content outside lawful authority and the approved process.

Annex F Technical information sharing record

Use for external drawings, software, process data, models and digital twin access.
Review derived information and embedded history as well as the visible file.

Record field	Required entry and evidence
Business purpose	Identify project, deliverable, recipient organisation and accountable asset owner.
Rights and conditions	Link permission to share, third party rights, confidentiality, allowed analysis and resulting intellectual property terms.
Information package	List exact files, versions, classification and the reason each item is necessary.
Recipient verification	Record named recipients, approved roles, trusted contact verification and subcontracting conditions.
Access controls	Specify channel, authentication, view or download rights, onward sharing limits and expiry.
Independent check	Confirm correct package, recipient, authority and absence of unrelated restricted information.
Release evidence	Record transmission date, package identity, receipt and accepted conditions.
Engagement closure	Reconcile deliverables, retained copies, rights, access removal and return or deletion evidence.

Do not treat a general cooperation agreement as permission for unrestricted sharing.
Preserve legitimate safety, compliance and service access through defined arrangements.

Annex G Prototype tooling and sample custody

Use for each uniquely identified asset or controlled group whose individual items remain traceable. Record custody changes at the time they occur.

Record field	Required entry and evidence
Asset identity	Enter prototype, tool, sample or media identifier, configuration, owner and classification.
Permitted purpose	State testing, repair, display, production or other authorised use and prohibited out of scope activities.
Release condition	Record condition, contents, embedded data, photographs where suitable and protective packaging.
Recipient and carrier	Verify receiving custodian, location, transport provider and approved subcontracting.
Handover trail	Record sender, receiver, time, condition, seals where used and proof of receipt.
Use and changes	Log testing, repairs, copying, destructive work, derived results and unexpected custody events.
Return or disposal	Reconcile items, remnants, data, approved retention and safe destruction or reuse evidence.
Exceptions	Identify missing items, damage, suspected exposure, legal holds and authorised closure decisions.

Sanitisation shall not invalidate a test or remove evidence needed for safety and compliance. A disposal certificate shall be assessed against the actual provider and method.

Annex H Role change and offboarding checklist

Coordinate Human Resources, the manager, Purchasing and access administrators.
Verify removal across physical and digital environments.

Record field	Required entry and evidence
Lifecycle event	Record role change, employment end or contract completion, effective time and authorised notification.
Responsibility transfer	Assign ownership of projects, records, service accounts and ongoing obligations to named custodians.
Physical assets	Reconcile badges, keys, devices, tools, documents, prototypes and loaned equipment.
Digital permissions	Review directory, repositories, cloud shares, supplier portals, remote access and local system rights.
Credentials and secrets	Assess exposed shared credentials, tokens and recovery information; record necessary rotation without exposing the secrets.
External copies	Confirm contractual return, deletion or permitted retention of information and derived results.
Verification	Record actual deactivation checks, administrator, time and any access remaining for an authorised reason.
Records and holds	Preserve required safety, quality and investigation records; apply privacy and retention rules to personal data.

Do not erase evidence needed for a legal hold. Access restrictions shall not obstruct protected reporting or lawful rights to relevant personal records.

Annex I Incident and evidence custody record

Open when a credible security event requires assessment. Preserve the difference between observed facts, reported claims and unresolved assumptions.

Record field	Required entry and evidence
Initial report	Record reporter channel, discovery time, location, affected assets and immediate safety concerns.
Triage	State verified facts, uncertainty, potential impact, incident lead and required specialist functions.
Containment	Record actions, authority, operational effects and the reason each measure was proportionate.
Evidence collection	Identify source, collector, time, method, original location and applicable legal or privacy limits.
Integrity and custody	Record evidence identifier, integrity checks where suitable, transfers, access and working copies.
Investigation	Link questions, alternative explanations, interviews, findings and independent review where required.
Disclosures	Record applicable notification assessment, verified deadlines, recipients, approvals and actual communications.
Recovery and closure	Confirm restored integrity, access review, corrective action, residual uncertainty and retention or hold decisions.

Emergency rescue takes priority over evidence collection. Do not conduct unauthorised personal searches, interception or property seizure under this form.

Annex J Monitoring and privacy assessment

Complete before introducing or materially changing cameras, biometrics, access analytics or data loss monitoring. Reassess when purpose or technology changes.

Record field	Required entry and evidence
Purpose	Define the specific protective need, affected assets and why the proposed measure is necessary.
Alternatives	Assess less intrusive options and explain the selected scope using documented risk.
People and data	Identify affected groups, data elements, sensitivity, collection locations and possible incidental capture.
Lawful process	Record Legal and Privacy review, required notice, consultation and any restrictions on use.
Access and security	Define who can view, export or investigate results and how access is logged and protected.
Retention	Set justified retention, review events, deletion controls and legal hold handling.
Alert fairness	Define contextual review, false positive handling, correction routes and separation from unrelated employee evaluation.
Effectiveness review	Record tests, complaints, incidents, changed risks and the decision to continue, modify or discontinue the measure.

A tool's capability does not establish permission to use it. Monitoring shall remain proportionate, transparent where required and limited to authorised purposes.

Annex K Worked access and custody metrics

Illustrative management exercise. These figures define no universal service deadline or acceptable security failure rate.

Record field	Required entry and evidence
Review population	Assume 240 active restricted access grants are due for review during the chosen period.
Recorded completion	Owners return 216 reviews. Administrative completion is 216 divided by 240, or 90 percent; 24 remain overdue.
Substantive result	The 216 reviewed grants include 18 rights no longer needed. Completion alone therefore does not demonstrate appropriate access.
Corrective action	Remove the 18 rights through the approved process and investigate why the lifecycle controls did not remove them earlier.
Custody population	A programme has 35 external prototype loans. Thirty two are reconciled and 3 lack current custody confirmation.
Interpretation	Reconciliation is 32 divided by 35, approximately 91.4 percent. Each of the 3 unresolved loans still requires individual risk assessment.
Management decision	Assign owners, verify asset sensitivity and current custody, and escalate based on actual exposure rather than the percentage alone.
Effectiveness check	Review subsequent lifecycle events and loan handovers to determine whether the underlying process has improved.

Keep simulated data separate from live records. Do not set targets that encourage staff to close reviews or incidents without evidence.

Annex L Contractor disclosure and recovery exercise

Run a coordinated exercise with a sponsor, Security, Engineering, Information Security, Operations, Legal and Privacy. Use fictional information and authorised simulation methods.

Record field	Required entry and evidence
Initial situation	A contractor is approved to diagnose one production cell during a defined support window.
First inject	The contractor requests a complete programme library and photographs a screen containing an unrelated prototype identifier.
Second inject	Monitoring reports a large download from the sponsor's shared folder; an approved backup may explain part of the activity.
Third inject	The sponsor is absent, production is stopped and a manager asks for unrestricted remote access to accelerate recovery.
Required decisions	Verify scope, preserve facts, distinguish authorised work from exposure and provide controlled urgent access if justified.
Expected records	Produce a scope change decision, sharing record, incident triage, evidence log and temporary access closure.
Evaluation	Check safety, proportionality, absence of premature accusations, asset integrity and traceability of information actually shared.
Improvement plan	Assign actions for unclear permissions, excessive shared folders, sponsor deputies and weak emergency access arrangements.

The exercise shall not involve real unauthorised intrusion or covert monitoring. Success means a defensible response that protects assets while preserving safe operations and fair treatment.