

IDM UID <b>S3893D</b>
VERSION CREATED ON / VERSION / STATUS <b>05 Oct 2018 / 3.1 / Approved</b>
EXTERNAL REFERENCE / VERSION

## MQP Procedure

# ITER Site access Procedure

This procedure describes the process to be followed in order for access to the ITER Site to be granted.

<i>Approval Process</i>			
	<i>Name</i>	<i>Action</i>	<i>Affiliation</i>
<i>Author</i>	<b>Peaucelle X.</b>	<b>05 Oct 2018:signed</b>	<b>IO/DG/RCO/SD/SHS</b>
<i>Co-Authors</i>	<b>Rouxel E.</b>	<b>05 Oct 2018:signed</b>	<b>IO/DG/RCO/SD/SHS</b>
<i>Reviewers</i>	<b>Cruceana I.</b>	<b>08 Oct 2018:recommended</b>	<b>IO/DG/CAB</b>
	<b>Flament F.</b>	<b>16 Oct 2018:recommended</b>	<b>IO/DG/RCO/FPD/PCD</b>
	<b>Frentz G.</b>	<b>08 Oct 2018:recommended</b>	<b>IO/DG/RCO/HRD</b>
	<b>Miele P.</b>	<b>09 Oct 2018:recommended</b>	<b>IO/DG/RCO/PCO/CDPC</b>
	<b>Ramu C.</b>	<b>09 Oct 2018:recommended</b>	<b>IO/DG/RCO/SD/SHS</b>
	<b>Schmieder L.</b>	<b>09 Oct 2018:recommended</b>	<b>F4E</b>
	<b>Tada E.</b>	<b>09 Oct 2018:recommended</b>	<b>IO/DG/RCO</b>
	<b>Tyler A. *</b>	<b>08 Oct 2018:recommended</b>	<b>IO/DG/CAB/LGA</b>
	<b>van Baaren W. *</b>	<b>16 Oct 2018:recommended</b>	<b>IO/DG/COO/CST/FLM/FMM</b>
	<b>Zhao Z.</b>	<b>14 Oct 2018:recommended</b>	<b>IO/DG/QMD</b>
<i>Approver</i>	<b>Bigot B.</b>	<b>18 Oct 2018:approved</b>	<b>IO/DG</b>
<i>Document Security: Internal Use</i> <i>RO: Fabre Nadine</i>			
<i>Read Access</i>	<b>LG: Quality Control Group, AD: ITER, AD: External Collaborators, AD: IO_Director-General, AD: EMAB, AD: OBS - Quality Management Division (QMD) - EXT, AD: OBS - Quality Management Division (QMD), AD: Auditors, AD: ITER Management Assessor, project administrator, RO, AD: OBS - Construction Management...</b>		

*Change Log*

**ITER Site access Procedure (S3893D)**

<i>Version</i>	<i>Latest Status</i>	<i>Issue Date</i>	<i>Description of Change</i>
v0.0	In Work	15 Oct 2015	
v1.0	Approved	20 Apr 2016	First issue, document created as per MQP doc Request RW3B22
v2.0	Signed	27 Oct 2017	Update following new organisation. Security file modified by Access Request Information Form. Workflow modified. Update granted as per MQP doc Request UVRAXH
v2.1	Approved	10 Nov 2017	Integration of Guillaume Frenzt comments with his formal agreement. A follow up version will be made later once SHS Data protection document is approved in order to reference this document.
v3.0	Signed	26 Sep 2018	major version as per approved MQP doc Request - WTDZGU. Main changes: Simplification and clarification as per RoD of MQPWG (ITER_D_WQDZ63) * extract technical details How to request access to and within the ITER Site - ITER_D_WRWQRG * implementation a Level 3 describing the management of access for specific areas - ITER_D_X3P7FQ * integration of minor comments from pre-review
v3.1	Approved	05 Oct 2018	This minor update takes into account the comments made on v3.0 by Anna TYLER, Zhanwei ZHAO and Guillaume FRENZT. The minor changes include: - The reference to 2LL5AM has been deleted from the flowchart. - The definition of "Submitter" has been re-worded following suggestions from the QARO and Anna TYLER. The changes are slight. - Other minor wording changes have been integrated following Anna TYLER's useful comments on v3.0 and the articles of the Labour Code have been adjusted.

## Contents

<b>1</b>	<b>PURPOSE .....</b>	<b>2</b>
<b>2</b>	<b>SCOPE.....</b>	<b>2</b>
<b>3</b>	<b>DEFINITIONS AND ACRONYMS .....</b>	<b>2</b>
	3.1 DEFINITIONS .....	2
	3.2 ACRONYMS .....	3
<b>4</b>	<b>REFERENCE DOCUMENTS .....</b>	<b>3</b>
<b>5</b>	<b>BASIC PRINCIPLES.....</b>	<b>4</b>
	5.1 GENERAL OVERVIEW .....	4
	5.2 PRINCIPLES RELATED TO THE CONTEXT OF THE ACCESS REQUEST .....	4
	5.3 PRINCIPLES RELATED TO THE PRE-ENROLMENT APPLICATIONS.....	5
	5.4 PRINCIPLES RELATED TO BADGE ISSUANCE AND THE USE OF BADGES.....	5
<b>6</b>	<b>WORKFLOW.....</b>	<b>6</b>
<b>7</b>	<b>OUTPUTS .....</b>	<b>8</b>

# 1 Purpose

The purpose of this procedure is to establish the general responsibilities related to ITER Site access and the general rules to be applied in order to access the ITER Site.

# 2 Scope

This Level 2 document falls under the Integrated Safety, Environment and Security Management System (ISMS) [1] in the scope of the Security process.

This procedure defines the general rules for site access to be complied with by any individual requesting access to the ITER Site or to any area within the ITER Site. Further detailed specific rules pertaining to site access, or access to any area within the ITER Site, are included in [2].

Access rules for vehicles on the ITER Site are detailed in another specific procedure [3].

# 3 Definitions and acronyms

## 3.1 Definitions

- **ITER Site** – “ITER Site” refers to the configuration of the ITER Site as defined in the ITER Site Master Plan [4].
- **Installation** – As defined in [5].
- **Identity document** – “Identity document” refers to a national identity card (for European citizens only), a French Titre de Séjour or a passport. For the execution of this document, no other forms of identity document, such as driving licences, are accepted.
- **The badge holder** – “The badge holder” refers to the person in possession of a valid ITER Site access badge.
- **The applicant** – “The applicant” refers to the person who requires access to the ITER Site, or an area within the ITER Site, and for whom an access request is submitted.
- **The Submitter** – “The Submitter” refers to the person who initiates an access request as shown in the first column of Figure 1. The Submitter is a relevant person identified and authorized by SHS and can be:
  - An IO Staff member such as the Responsible Officer (RO) as defined below
  - An employee of any legal entity involved in the ITER Project
  - Or a member of the Human Resources Department as defined in [2LL5AM](#).The applicant cannot be the Submitter.
- **The Responsible Officer** – “The Responsible Officer” (RO) refers to the IO Technical Officer appointed by management as the person responsible for an IO process or for the technical aspects of full-cycle contract performance including initiating the procurement request, preparing the technical specifications, and being the IO’s single point of accountability for the overall technical execution of a contract.
- **The Reviewer** – “The Reviewer” refers to a person who reviews an access request as shown in the second and third columns of Figure 1. The Reviewer may be an Occupational Health & Safety (OHS) Reviewer (see below), an IO staff member (such as the Submitter’s

line manager, the Chief of Installation or the contract RO), or an employee of any legal entity involved in the ITER Project.

- **The OHS Reviewer** – “The OHS Reviewer”, as shown in column two of Figure 1, reviews OHS aspects of access requests depending on the area requested and the activities to be performed (see 5.2).
- **The Approver** – “The Approver” refers to the final person in the access request approval workflow as shown in the fourth column of Figure 1. The Approver is any relevant person identified and authorized by SHS.
- **Pre-enrolment application** – “The pre-enrolment application” refers to the computer program used to submit and treat access requests for the ITER Site or for any area of the ITER Site that is identified and registered in it.
- ITER security definitions ([7GH8F5](#))

### 3.2 Acronyms

- ITER Abbreviations ([2MU6W5](#))
- ITER Occupational Safety Abbreviation ([S97BRM](#))
- **DA** = Domestic Agency
- **HSPC** = Health and Safety Protection Coordinator
- **IO** = ITER Organization
- **OHS** = Occupational Health & Safety
- **RO** = Responsible Officer
- **SHS** = Security, Health and Safety Division

## 4 Reference Documents

- [1] ITER Integrated Safety, Environment and Security Management System (ISMS) Manual ([4HCWJU](#))
- [2] How to request access to and within the ITER Site ([WRWQRG](#))
- [3] Vehicle Access and Traffic Circulation and Parking on the ITER Site ([N3MG3V](#))
- [4] ITER Site Master Plan ([27X5FM](#))
- [5] General Instruction Note n° 006 - Role of the Chief of Installation ([UFF9DT](#))
- [6] Working Instruction for the Management of Area Access “How-To” Documents ([X3P7FQ](#))
- [7] Site Plan for Internal Regulations ([RZGQKW](#))
- [8] [French Labour Code](#)
- [9] [French Defence Code](#)
- [10] Internal Regulations ([27WDZW](#))
- [11] PGC SPS Vol. 1 – IO&F4E ([T6V4RP](#))
- [12] ITER Site Pass-Loss/Theft Report ([7M4GT7](#))
- [13] Staff Regulations of the ITER Organization ([2EFKUE](#))
- [14] ITER Site Protection Enforcement Rules ([V9ZWCA](#))
- [15] SHS Data Protection Guidelines ([WT7JUL](#))

## 5 Basic principles

### 5.1 General overview

Access to the ITER Site shall entail the following steps:

- The definition of the context of the access request including:
  - The reason for which the applicant requires access to the ITER Site
  - The required area(s) and ITER Site entrance(s)
  - The required duration of the on-site presence.
- The use of the appropriate pre-enrolment application.
- The issuance of the badge associated with the implementation of the required access rights and the correct use of the badge.

Any person responsible for an area as defined in 5.2 (e.g. “Chief of Installation” [5]) should detail access rules for said area (e.g. installation) following the principles detailed in [6].

Under the Director-General’s responsibility, the principles mentioned below shall apply throughout this process. Detailed information related to access control can be found in [2].

### 5.2 Principles related to the context of the access request

- Access to the ITER Site shall be strictly for professional reasons with the exception of special events organized by the IO such as Family Lunch Day, ITER Open Days or school visits.
- The minimum age limit for a person accessing the ITER Site is 18 years excluding special events organized by the IO such as ITER Open Days, Family Lunch, school visits or special educational programs.
- Company identification details, supported by the relevant valid legal and contractual documentation, shall be registered in the appropriate pre-enrolment application for any Contractor/Subcontractor involved in the ITER Project that requires access to the ITER Site for its personnel. This information justifies that the concerned legal entity is registered and is administratively and legally reliable.
- The ITER Site is organized on the basis of areas<sup>1</sup>. These areas and the various ITER Site entrances are identified in the Site Plan for Internal Regulations [7].
- Access to any area on the ITER Site is regulated and restricted. No one can access the ITER Site or an area within the ITER Site without authorization from the designated authority.
- Depending on the activities undertaken in an area, it is regulated by either:
  - Articles L.4531-1 to L.4535-1 and R.4532-1 to R.4535-13 of the French Labour Code [8] hereafter referred to as “Decree 94”.
 Or:
  - Articles L.4511-1 and R.4511-1 to R.4515-11 of the French Labour Code [8] hereafter referred to as “Decree 92”.

The areas of the ITER Site that fall under the legal framework of Decree 92 and Decree 94 are defined in the Site Plan for Internal Regulations [7].

- OHS aspects depending on the area requested and the activities to be performed shall be identified and appropriate legal and contractual documents shall be established.
- The various ITER Site entrances are each associated with specific areas. The ITER Site entrance to be used may be dictated by the specificity of the area to be accessed. Individuals with access rights to various areas may automatically have the right to cross certain internal gate/s.
- The duration of the on-site presence shall not exceed that which is strictly necessary.

---

<sup>1</sup> An area could be an “Installation” in the meaning of [5] **Error! Reference source not found.**

### 5.3 Principles related to the pre-enrolment applications

- An access request shall be submitted through the appropriate pre-enrolment application for any person requiring access to the ITER Site, or any area within the ITER Site identified in the application, in order for access rights to be granted.
- Users of the pre-enrolment applications shall respect the following rules,:
  - The applicant shall not be the Submitter
  - The Reviewer shall not be the Submitter
  - The Approver shall not be the either the applicant, the Submitter or the Reviewer.

The main responsibilities of the Submitter, Reviewer and Approver are listed in Figure 1 and further information is provided in [2].

- Access requests in the pre-enrolment application follow a specific, pre-defined access request approval workflow (Figure 1) which involves the participation of a minimum of two people (not including the applicant) in order to ensure the separation of duties.
- Certain mandatory documentation and information (e.g. personal or contractual information/documentation) may be required.

The access request approval and badge issuance process may differ depending on the area requested and its applicable laws and regulations (as defined in 5.2) in addition to the activities to be performed.

- A Submitter shall only submit access requests for the professional purpose of their own department<sup>2</sup>.
- The access request approval process from Submitter to Approver shall be completed within the timeframe specified in [2]. If this timeframe is not respected, the request will be subject to a specific approval workflow which includes the implication of upper level management such as, for IO, the Director-General, Deputy Director-General or a Head of Department (see [2]).
- Access requests shall only be validated by SHS or the Reception Offices as applicable.

### 5.4 Principles related to badge issuance and the use of badges

- The IO has the authority to refuse or withdraw access rights at any time. The concerned parties are informed.
- SHS shall carry out regular audits of the entire access control process.
- Any person requesting access to the ITER Site may be subject to a background check by the Host State's relevant authorities under the provisions of Article L.1332-2-1 of the Defence Code [9]. Depending on the result of such a background check, specific access conditions may be put in place or access to the ITER Site denied.
- Any person undertaking activities on the ITER Site is subject to the Internal Regulations [10].
- For access to areas under the legal framework of Decree 94 [8], badge issuance and validity shall rely on the fulfilment, by the applicant, of the measures related to safety awareness defined in [11] and detailed in [2]. All access rights to areas under the legal framework of Decree 94 will be blocked until these measures are met.
- The following access badge conditions of use shall apply in any case:
  - The badge shall be presented to the security guard and/or to an area's Access Control System electronic badge reader upon entering and exiting the ITER Site or upon request.
  - Within the ITER Site, a valid badge must be worn in a visible manner at all times and may be checked in any area.

---

<sup>2</sup> For the purpose of this document, "department" means Department, Office, or other equivalent organizational unit.

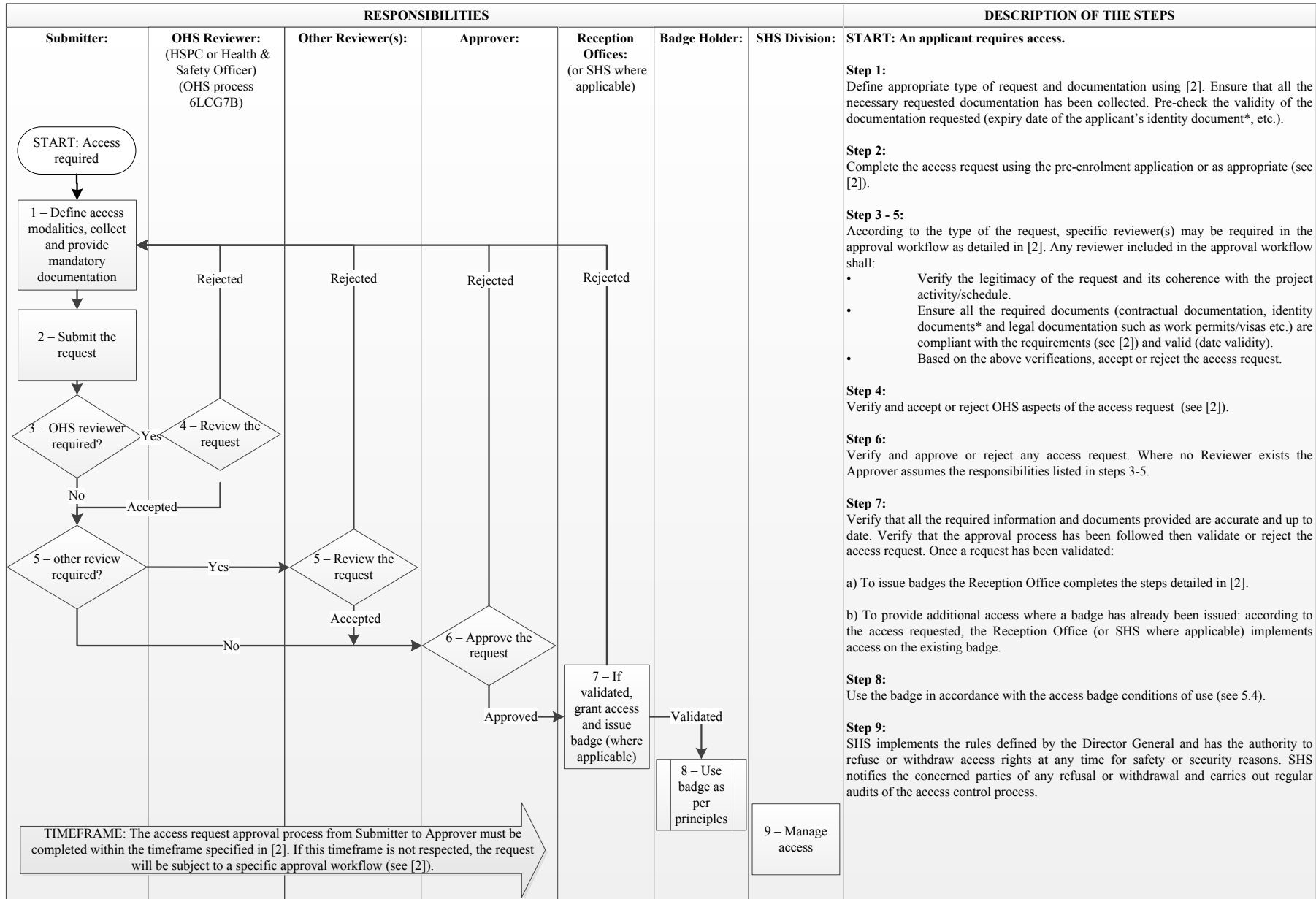
- Outside the ITER Site, badges should not be visible and should be hidden away.
  - Affixing a sticker to a badge is strictly forbidden without prior authorization from SHS.
  - The badge is non-transferable. It is strictly forbidden, under any circumstances, to lend or transfer a badge to another person. The copying, cloning or reproduction of badges is also strictly forbidden.
  - Should a badge be forgotten, the badge holder must go the Reception Office in order to be granted a temporary badge. The forgotten badge shall be temporarily deactivated. On presentation of a valid identity document, a temporary replacement badge can be issued. This temporary replacement badge must be returned as per the instructions provided by the Reception Offices or guards.
  - Should a badge be lost or stolen, the badge holder must immediately report it to the Reception Offices during site opening hours or to the Security Command Post (available 24/7 by telephone) outside opening hours.
  - For badges reported as lost or stolen, a loss/theft report [12] shall be completed at the Reception Offices by the badge holder. The badge reported as lost/stolen shall be immediately deactivated. On presentation of a valid identity document, a replacement badge can be issued for a period defined in [2].
  - Badge holders must return their badges to the Reception Office or to the Guardhouse as soon as their contract, mission or on-site visit is finished. When a permanent badge holder leaves the ITER Site definitively, their employer or manager shall inform the Reception Office and can be held liable if his/her badge is not returned.
- Any staff member in breach of his/her obligations under these principles may be subject to disciplinary measures under Article 23 of the Staff Regulations [13] or according to [14]. Infractions by non-staff members shall be addressed according to [12] and/or directly with the person's employer.
  - The maximum length of validity of access badges shall depend on the status of the applicant and the purpose of their onsite presence.
  - Access badges shall be issued exclusively under the authority of SHS.
  - Access badges can be issued only once the approval workflow has been correctly completed and the request has been validated by SHS or the Reception Offices.
  - In some cases, identity documents may be kept in exchange for access badges.
  - Access badges shall have different visual aspects which allow for the verification of security elements and information related to the onsite presence of the applicant.

## 6 Workflow

The flow chart below (Figure 1) describes the access request approval workflow, its interactions with other MQP documentation, and the responsibilities of those involved.



Figure 1



\* See 3.1 Definitions for acceptable identity documents.

## 7 Outputs

Records related to Access Control are managed in accordance with the SHS Data Protection Guidelines [15].

The execution of this document requires the following outputs:

Type of output	Format (Template, form, checklist)	Location of output	Document type	Instructions for identification of the output	Responsible for managing the output	Retention period
<i>Access request</i>	<i>Online form</i>	<i>Stored in IDM</i>	<i>Access request</i>	<i>Assigned automatic UID in IDM, can be searched for using the applicant's name</i>	<i>SHS Division Head</i>	<i>As per [15]</i>
<i>ITER Site Pass Loss/Theft Report (Record)</i>	<i>Form [12]</i>	<i>Stored in a physical folder in the Reception Office</i>	<i>[D]-Form. Archived as a paper form.</i>	<i>N/A</i>	<i>SHS Division Head</i>	<i>As per [15]</i>
<i>Documentation uploaded to the access request in the pre-enrolment application such as: Identity documents etc.</i>	<i>French ID Card (CNI), European ID card (CIE), French Titre de Séjour or Passport</i>	<i>Stored within the access request in the pre-enrolment application</i>	<i>Archived as a pdf, jpeg or png file.</i>	<i>No specific instructions as the file is attached directly to the access request which is identified by UID and name of the applicant.</i>	<i>SHS Division Head</i>	<i>As per [15]</i>