Application for a Security Clearance

Important to note: *This form needs to be completed by the line manager who applies for a security clearance on behalf of an employee/contractor and should be submitted with the completed Z204 security clearance application form of the State Security Agency (SSA) or the DD1057 security clearance application form of Defence Intelligence (DI), whichever is applicable.*

A copy of this form will be provided to the applicant as evidence that a security clearance application form and supporting documentation was submitted and will also serve to confirm the grade of clearance that was applied for. Please keep this form in a safe place for future reference.

Security Vetting is exempted from Protection of Personal Information Act 4 of 2013, par 6(1)c, as it is performed by the SSA for purposes of national security. The information collected will be processed with the highest level of confidentiality.

1. Details of applicant SSA

Employee number	109884
Full names and surname	Pontsho Lindiwe
Position currently occupied	Software Developer
Project number	26273
Telephone number	0763364622

2. Details of line manager

Employee number	108396
Full names and surname	Lavhelesani Marcia Muthakhi
Position currently occupied	Software Developer
Cost Centre number	21650
Project number	26273
Telephone number	0152978167

3. Details of clearance required

Please indicate which grade of clearance is required. Mark with "X".	**Confidential Clearance**	**Secret Clearance**	**Top Secret Clearance**
Motivation for grade selected (one sentence will suffice): SITA Employee works on Government Departments networks			
Note: *1. If uncertain about the required grade of clearance, please review the attached guideline or contact the Security Vetting Department.* *2. The cost of the clearance, as published in the annual budget guidelines, will be recovered from the applicable project upon submission of the application.*			

Signed by Line Manager: _____ Requested date: 2024/ 07 /

Application accepted by Security Vetting Services (For internal use only)	
Name and surname	
Position	
Date received	
Outstanding documents	
Date on which outstanding documents are submitted	
Signature	

Which grade of security clearance is required for me?

The question most often asked when completing a security clearance application form is what grade of clearance is required i.e. confidential, secret or top secret. This 3 page document aims to assist the applicant and line manager with answering this question and also aims to provide a framework in which the correct decision can be made.

1. Definitions

Let's start by examining the only official definitions for the three security clearance grades and translate it to our organisation. The Minimum Information Security Standards, often referred to as the *"MISS"*, is a Cabinet approved policy document on information security in the public service and the only document defining the clearance levels or grades. According to the MISS, the three grades of clearances are defined as:

1.1 **Confidential:** *"Classification limited to information that may be used by malicious/opposing/hostile elements to **harm** the objectives and functions of an organisation and/or State"*.

Translation: Confidential information can also be referred to as company confidential information and includes projects, processes and systems that are used in the organisation in executing its strategic objectives. Each and every employee in the organisation will have access to this type of information because it also refers to the institutional knowledge of the organisation, policies, procedures as well as the culture i.e. the way we do things at SITA. Lastly, some SITA buildings have been classified as National Key Points, as provided for in the National Key Points Act. If a SITA employee or contractor has access to these buildings, a security clearance is required.

1.2 **Secret:** *"Classification given to information that may be used to **disrupt** the objectives and functions of an organisation and/or State".*

Translation: Secret information is regarded as very sensitive and if not effectively managed may disrupt the functioning of the organisation through industrial action, disruption or neutralisation of business relationships, de-motivated staff, poor performance and the failure of projects. It is also important to note that information contained on the systems of certain key SITA clients can also be classified as secret. Employees and contractors with access to these systems, or the programme code behind it, must therefore apply for a secret clearance.

1.3 **Top Secret:** *"Classification of information that can be used to **neutralise** the objectives and functions of an organisation and/or State".*

Translation: Top secret information is extremely sensitive and if not managed effectively may cause a severance of diplomatic ties, declaration of war or neutralisation of an organisation – in our case, SITA. Any information that will permanently damage the relationship that the company has with its sole stakeholder, Government, will be regarded as top secret since the misuse of this information may lead to the neutralisation of the organisation. It is also important to remember that the employee or contractor might not necessarily have access to top secret SITA information but that he/she might have/gain access to top secret information of the client, such as SAPS, DoD, Treasury etc.

2. Roles and responsibilities

As contained in the Vetting Policy, the responsibility and accountability of the vetting process lies with Vetting Services as well as with line management. The separate roles and responsibilities can be broken down as follows:

2.1 Vetting Services

Vetting Services at SITA is responsible for the overall management of security clearances within the organisation. The following can be regarded as its key roles and responsibilities:

a) Conduct vetting fieldwork on all security clearance applications according to the MoU between SITA and the State Security Agency (SSA);
b) Keep record of all the security clearance statuses for each and every employee through an effective administration system;
c) Liaise with the SSA and Defence Intelligence (DI) on processes, systems, vetting criteria and issued clearances;
d) Create awareness and education on obtaining and maintaining a valid security clearance;
e) Upload all clearance application data to the SSA vetting system;
f) Provide guidance to line management in terms of security clearance processes, grades and validity periods;
g) Ensure compliance to the Vetting policy at all times.

2.2 Line Management

As far as security clearances are concerned, line management is responsible for the following:

a) Liaise with the client to determine the grade of clearance required for all jobs under his/her supervision;
b) Ensuring that all employees apply for the correct grade of clearance;
c) Manage information security in the workplace;
d) Liaise with the Vetting Specialist allocated to his/her environment in order to obtain updated and current security clearance statuses for all staff;
e) Inform Vetting Services of any activity or behaviour that may affect an employee's security competency such a disciplinary action, financial difficulty, internal investigations or poor performance;
f) Comply with the Vetting Policy at all times.

3. THE ROLE OF VETTING SERVICES: DICTATING OR GUIDING?

It is very important to note that Vetting Services can only play a guiding role in determining the correct grade of clearance required and never a dictating one. A security clearance is in essence a measure implemented to protect the information of the organisation. It is therefore the responsibility of Vetting Services to conduct the security clearance screenings but the accountability for protecting the information of the organisation lies with line management and each and every employee. Vetting Services, as a business unit, cannot be held responsible if someone has access to information that he/she is not supposed to have - Vetting Services do not control access, line management does. The business must therefore dictate to Vetting Services in terms of which grade of clearance is required for each and every position and Vetting Services in turn will execute the applicable clearance process.

The argument that Vetting Services can only play a guiding or advisory role, when it comes to deciding which grade of clearance is required, is further supported by the following:

a) Vetting Services doesn't have direct contact with the client and therefore doesn't know what the client's unique security requirements are.
b) One size doesn't fit all when it comes to security clearances – a LAN Support Technician working for the DoD at Defence Head Quarters may require a *Top Secret* clearance whereas a LAN Support Technician working for the Department of Housing might only require a *Confidential* clearance. Line management should know what the client requirements are.
c) Line management controls access to information, Vetting Services doesn't. When it comes to Personal Assistants, for example, some managers provide more access than others – one manager might control access very vigilantly and ensures that his/her Personal Assistant only has access to confidential information while another manager might give his/her Personal Assistant access to all information and systems, which may requires a *Top Secret* clearance.
d) Line management is accountable for information security and can therefore make a decision that all LAN Support Technicians, as an example, be cleared to a specific level or all Call Centre Agents to another level. If such a decision is made, it will

be the responsibility of Vetting Services to implement an action plan that will ensure the speedy execution of the security clearances to the required levels.

4. CONCLUSION

The grade of security clearance required has nothing to do with the position the employee occupies or the level of that position in the hierarchy of the organisation. It has everything to do with the nature of the information that the employee has access to, the classification thereof (if any) and the requirement of the client when a SITA employee has access to external systems. It is very important to ensure that this distinction is made when deciding on which grade of clearance is required.

Line management needs to understand the information security requirements within each environment and decide on the appropriate clearance grade, with the guidance of Vetting Services.

General Enquiries	**Vetting Officer** **VD Mutswaletswale (0791857401)** **Vhonani.Mutswaletswale@sita.co.za**