TECHNICAL DESCRIPTION

Corporate Protection Against Internal Threats to Corporate Information Security

WorldSkills Russia "Young Professionals" Union (hereinafter referred to as WSR) in accordance with the charter of the organization and rules of the competition has established the following minimum requirements to this professional skill required for participation in the skill competitions.

The technical description includes the following sections:

1. INTRODUCTION

1.1. Profession (skill) name and description

1.1.1 Profession (skill) name:

Corporate Protection Against Internal Threats to Corporate Information Security

1.1.2. Profession (skill) description

Currently, one of the most relevant issues of corporate data security is ensuring the protection against internal leaks through technical communication channels. One of the main threats to corporate data security is the illegal activities of employees (so called insiders), resulting in the loss of confidential data, performed both intentionally and due to negligence, inattention or ignorance about basic rules of enterprise security. They are responsible for most of the notorious data theft cases, recorded throughout the world in the last few years. Leaks also may be caused by actions of third parties, present at the territory of the enterprise and having access to the computational network infrastructure (customers, suppliers, etc.). Information leaks may result in a number of problems:

1. Personal data leak. May result both in sanctions on behalf of regulatory authorities and in withdrawal of customers due to the loss of confidence in the company.

2. Leak of commercial secrets and know-how. The leak of information about investment plans, marketing programs, innovations, customer database data is capable of undermining important and profitable projects.

3. Leak of operational correspondence. Operational correspondence may provide a lot of information about the company's status to its competitors.

4. Leaks to the media. May result in the disclosure of the organization's business secrets.

5. Leak of information on the security system. Opens wide opportunities for activities of criminal structures.

6. Leak of data comprising a state secret, etc.

The need for protection against internal threats to information security has not only been proven in practice, but also has been mentioned in critical international standards on information security organization and management (e. g. in ISO/IEC 27001).

Technologies of corporate protection against internal threats to information security, attributed to the Data Leak Prevention (DLP) class, allow identifying and preventing the leaks of confidential information and personal data, protecting companies against fraud, theft and corruption, detecting illegal actions of the employees as well as unauthorized use of corporate resources. Corporate security systems allow to clearly detect incidents and provide the entire set of tools to carry out internal investigations and the subsequent legal protection of corporate interests.

Experts in corporate security must possess theoretical knowledge on provision of corporate protection against internal threats, understand the aspects of application of the regulatory legal base to classification and investigation of incidents, be proficient in the use of systems and techniques provided for achievement of protection purposes.

An integral part of works aimed at ensuring corporate security against internal leaks is performing the entire set of technical operations for data flow analysis, both those circulating within the perimeter of the secure information system and those crossing it. For this purpose, experts must be able to conduct the entire cycle of works for installation, deployment, adjustment, use of DLP systems, including the development of information security policies, classification of protection objects, application of filtration techniques to various types of traffic, filtration of the intercepted traffic to search for identified incidents, issuing the permit/prohibition for delivery of certain data, analysis of the contents of intercepted traffic to disclose violations of the corporate security policy, diagnostics of the working capacity, etc.

An expert in corporate security prepares and submits reports on the identified incidents (along with his assessment of the threat level and regulatory evaluation) to the management of the protected organization.

1.2. Scope of application

1.2.1. All experts and competitors must become closely familiar with this Technical Description.

1.2.2. In case of inconsistencies between different translations of the Technical Description, the Russian language version will have a higher priority.

1.3. Supporting documents

1.3.1. The Technical Description only covers professional matters. It shall be studied together with the following documents:

- WorldSkills Russia, Competition Standing Orders;
- WorldSkills International, WorldSkills Russia: online resources listed in this document;
- OHSE rules and sanitary standards.

2. QUALIFICATION AND SCOPE OF WORK

The competition is aiming at demonstrating and evaluating of the skill qualifications. Test Project is exclusively practical.

2.1. Qualification requirements

The competitors must possess the knowledge and understanding of the following aspects, bearing in mind the fact that the test project may include any of the following knowledge elements.

2.1.1. Work organization and management

Knowledge and understanding of:

- Working principles of an information security specialist and their practical application;
- Safe operation principles and regulations as a whole and with regard to corporate environment;
- Regulatory documents in the sphere of information system security;
- Regulatory documents in the sphere of OHSE;
- Importance of labor organization in accordance with the methods;
- Research methods and techniques;
- Importance of management of personal professional development;
- Rate of changes in the IT and information security sectors, as well as importance of conformance to the modern-day level.
- Importance of the ability to listen to the interlocutor as a part of effective communication;

- Roles and requirements of colleagues and most effective communication methods;
- Importance of building and maintaining productive working relations with co-workers and supervisors;
- Methods of resolving misunderstandings and conflicting demands;
- Methods of stress and anger management for resolution of difficult situations.

Skills:

- Maintain a safe, neat and effective work booth;
- Use all equipment and software in a safe manner and in accordance with manufacturer's instructions;
- Follow the requirements in the sphere of OHSE;
- Plan personal work and adjust plans in accordance with changing priorities on a regular basis;
- Maintain the workstation in good condition and order.
- Demonstrate the well-developed ability to listen and ask questions to achieve a deeper understanding of complex situations;
- Build the effective written and oral communication;
- Understand the changing demands and adapt to them;

2.1.2. Installing, configuring and eliminating the faults in the system of corporate protection systems against internal threats

Knowledge and understanding of:

- Network neighborhood;

- Network protocols;
- Know the methods of identifying and building the paths of information movement within the organization;
- Approaches to building a network and how network devices can be adjusted for effective interaction;
- Types of network devices;
- Diversity of operating systems, their capabilities from the perspective of their use by users and for deployment of components of protection systems against internal threats;
- The process of selection of appropriate drivers and software for various types of hardware and operating systems;
- Importance of following instructions and the consequences, price of neglecting them;
- Precautions recommended to be made before installing software or updating the system;
- Stages of installation of the system of corporate protection against internal threats;
- Know the differences of various versions of systems of corporate protection against internal threats;
- Know what DBMS are supported by the system;
- Know the designation of different components of versions of systems of corporate protection against internal threats;
- Know the techniques of software and hardware virtualization;
- Know the characteristics of operation of principal hypervisors (monitors of virtual devices), such as VirtualBox, VMWare Workstation;

- Goal of documenting the processes of updating and installation.
- Importance of the calm and focused approach to problem solving;
- Importance of systems of IT security and dependence of users and organizations on their availability;
- Frequent hardware and software errors;
- Know the sections of the corporate security system, generally used by the system administrator;
- Analytical and diagnostic approaches to problem solving;
- Limits of personal knowledge, skills and authorities;
- Situations that require an intervention on behalf of the support service;
- Standard timeline of solving the most frequent problems.

Skills:

- Interpret user requests and demands from the perspective of corporate requirements;
- Utilize all types of configurations, software and hardware updates for all types of network devices that may occur within the network neighborhood;
- Adjust the network devices;
- Administration of automated technical tools for information and information flow management and control;
- Skills of system administration in Windows Server and Linux Red Hat Enterprise Linux operating systems;
- Installation of the server end of the system of corporate protection against internal threats;
- Installation of various DBMS;

- Installation of the agent end of the system of corporate protection against internal threats;
- Deployment of the guest virtual devices and their practical operation, using the latest hypervisors;
- Setting up individual components of the system of corporate protection against internal threats and the system as a whole;
- Use additional utilities, if required;
- Be able to check the system's working capacity and identify the faults, remove the problems and perform control checks;
- Approach the problem with the necessary confidence level in order to calm the user if necessary;
- Be able to configure the system to have it receive shadow copies;
- Regularly check the results of his/her own work to avoid problems at subsequent stages;
- Demonstrate confidence and persistence in resolving problems;
- Quickly recognize and understand the essence of faults and resolve them in the course of independent supervised work, accurately describe the problem and document its solution;
- Thoroughly investigate and assess the difficult, complex situations and problems, implement the troubleshooting methods;
- Select and accept the diagnostic software and tools for troubleshooting;

2.1.3. Inspection of the informatization object

Knowledge and understanding of:

- Typical staffing structures of organizations in various spheres of activity and sizes;
- Typical set of protection objects, information access priority, typical user roles;
- Data transmission channels: definition and types;
- Approaches to and methods of investigation of the informatization object for subsequent protection;
- Network devices that can be used as event sources for analysis;
- Generation of audit processes and procedures for information security.
- Inspection of corporate information systems.
- Status of corporate information.
- Tools and techniques of ensuring corporate protection against internal threats.
- Efficiency criteria of the project for ensuring corporate protection against internal threats.
- Obstacles to implementation of projects for ensuring corporate protection against internal threats.

Skills:

- Perform inspection of corporate information systems.
- Independently study the organization's structure based on received materials;
- Determine the protection objects, user roles, access rights;
- Identify data transmission flows and possible information leak channels;
- Create protection objects and the information security policy by using analysis techniques in the corporate security system;

- Based on the personal analysis, be able to connect the requirements of the regulatory base, organization's structure, detected threats, objects, security roles to build up-to-date security policies;
- Document and be able to present the results of inspection (audit), including data flows, potential leak channels, user roles, protection objects, etc.

2.1.4. Development of security policies within the system of corporate protection of information against internal threats

Knowledge and understanding of:

- Techniques of working with information security policies;
- Creating new policies, modifying the existing ones;
- General principles of working with the interface of the corporate information protection system;
- Protection objects, persons;
- Key techniques of traffic analysis;
- Typical protocols and data flows in the corporate environment, such as:
- corporate e-mail (SMTP, ESMTP, POP3, IMAP4 protocols)
- web mail;
- Internet resources: web sites, blogs, forums, etc. (HTTP, HTTPS protocols);
- social media;
- web messenger services; OSCAR (ICQ), Telegram, Jabber, XMPP, Mail.ru Agent, Google Talk, Skype, QIP;
- printers: printing files on local and network printers;
- any removable media and devices;

- Understanding the importance of the completeness of building the security policies to disclose all possible incidents and identify the leak occurrences;
- Types of threats to information security, types of incidents,

Skills:

- Create the maximum possible set of security policies in the system, covering all possible data transmission channels and possible incidents;
- Working with the technology section of the corporate protection system: categories and terms, text objects;
- Working with events, queries, interception objects, identification of contacts in an event;
- Working with summaries, vidgets;
- Working with persons;
- Working with protection objects;
- Performance of simulation of the confidential information leakage process within the system;
- Create consistent policies that conform to the regulatory base and the laws;
- Document the created policies, using in conformance with requirements of modern standards in the sphere of information security.

2.1.5. Technologies of network traffic analysis in the system of corporate protection of information against internal threats

Knowledge and understanding of:

- Traffic analysis techniques when working with information security policies within the corporate information protection system;

- Principal sections and operation characteristics of management of the corporate information protection system;
- Action algorithm when developing and using security policies based on various data analysis techniques;
- Typical signatures used to detect files that circulate in corporate information storage and transmission systems;
- Role of filters in the analysis of intercepted traffic; Technical restrictions of the filtration mechanism, its advantages and disadvantages;
- Sections of the corporate security system that are used by a security officer in the day-to-day work;
- Characteristics of processing HTTP queries and letters sent using web services;
- Corporate traffic analysis techniques, used in the corporate information security system;

Skills:

- Working with categories and terms;
- Using regular expressions;
- Using morphological search;
- Characteristics of the Linguistic Analysis technique;
- Working with graphics objects;
- Working with database uploads;
- Working with seals;
- Working with templates;
- Working with file types;

- Effectively use the filter creation mechanisms to assess the intercepted traffic and identified incidents;
- Perform the correct classification of the incident threat level;
- Use content filtration databases;
- Use additional modules for analyzing information flows, if this is dictated by the specific of doing business;

2.1.6. Agent monitoring techniques

Knowledge and understanding of:

- Agent monitoring functions;
- General settings of the agent monitoring system;
- Connection with the LDAP server and synchronization with Active Directory;
- Agent monitoring policies, characteristics of their setting;
- Characteristics of setting up agent monitoring events;
- Agent diagnostics mechanisms.

Skills:

- Installation and set-up of agent monitoring;
- Creation of agent-based protection policies;
- Operating an agent-management console;
- Event filtration;
- Setting up joint events of agent and network monitoring;
- Working with media and devices;
- Working with files;
- Application control;
- Exclusion from interception events.

2.1.7. Identified incident analysis. Report preparation, threat and incident classification

Knowledge and understanding of:

- Principal legal concepts and regulatory documents that govern the organization of corporate protection against internal threats in business entities;
- Tools, technologies, their sphere of application and restrictions when generating the corporate protection against internal threats;
- Standard package of regulatory documents required for deployment and operation of the corporate protection system within the company;
- Types of standard report forms about identified threats and incidents;
- Types of information security threats, understanding their urgency and level of the treat to a particular entity;
- Understanding approaches to investigation of the information security incident, methodology of threat level assessment;
- DLP systems and requirements for information security.
- Classification of information in the Russian Federation.
- Legal issues of DLP system use: personal or family privacy; communication secrecy; specific technical facilities
- Measures on ensuring DLP legitimacy (Pre-DLP).
- Law enforcement practices applied in the course of investigation of incidents related to internal information security procedure violation.

Skills:

- To develop regulatory and legal documents of the business entity related to arrangement of corporate protection against internal information security threats;
- To investigate internal information security incidents and draw necessary supporting documentation;
- To prepare reports on incidents, threats identified, etc.
- To submit reports to the management, to justify the analysis outputs.

2.2. Theoretical knowledge

Theoretical education is required but not subject to explicit assessment.

2.2.2 Knowledge of rules and regulations is taken into account

2.3 Practical work

Main Test Project

Participants should perform two Test Projects during 2 days' competition. Practical assignment is given in a form of TOR for corporate environment protection against internal threats. A competitor must perform the examination and analysis of the entity's structure (as the principal security object) based on the provided materials and the stand, its computational network infrastructure, determine data flows, potential threats and leakage channels. Technical part of work includes deployment, configuration and phased operation of the internal threats protection system to identify information leakage channels and other security incidents.

Identified incidents should be duly analyzed and classified according to existing regulatory framework. A level of information security threat should be assessed.

Results of work should be provided in a form of reports. Before putting protection technical system in operation, a set of documents regulating its legal use by the entity should be prepared. TOR consists of the entity's legend, its computational and network infrastructure specifications, as well as description of the technical facilities used.

Description of the entity, which is protected by competitors, includes:

- description of organizational and manpower structure of the entity;
- description of computational and network infrastructure;
- entity's internal documentation set;

Assessment of practical work is mainly aimed at assessing the result of the work, rather than the process. In the meanwhile, Test Project assessment criteria are drawn up in such a way that the optimal design, planning, installation, analysis and operation process of the projected protection system leads to a high score.

Supporting documents

Supporting documentation is prepared by competitors in the course of the competition and includes:

- Reports;
- Specifications;
- Presentations to upfold the work.

Scoring

Registration and counting all scores on main Test Project assignment is performed by the competition information system (CIS).

3. TEST PROJECT

3.1. Test Project format and structure

The Test Project consists of several separately assessed stages

3.2. Test Project requirements

The Test Project shall comply with the following requirements:

- Modularity;
- It should be supported by a special judgement form reflecting general assessment criteria and the number of points accumulated in the course of the competitions (Section 5);
- Comply with Item 3.5;
- Availability of all materials required for the work of experts at the competition site;
- Availability of all relevant documents and detailed manuals for a new and technologically sophisticated equipment and software;

3.3 Basic conditions for the proposed modules

Each module should:

- comply with the requirements of the Test Project development
- subject to fast translation into the competitor's language
- include brief description of the assignment

3.4 Main modules of the Test Project

Module	Module name	Time alloted for the

		module, hours
1.	**Installing, configuring and eliminating the faults in the internal threats corporate protection system**	**4**
	• Network infrastructure configuration: configuration of host computer, network environment, virtual machines etc.; • Installation and setting-up corporate system for protection against internal threats; • Self-search and troubleshooting during deployment and configuration; • Installation and set-up of agent monitoring; • Synchronization with the LDAP server is performed, the person's section is filled correctly; • Launch of the internal threats corporate protection system Performance of simulation of the confidential information leakage process within the system;	
2.	**Examination (audit) of the entity for internal threat protection**	**2**
	• Self-study the entity's structure based on the materials received ("organization model"), observe corporate information systems; • Identify the security objects; • Correctly formulate a list of subjects/persons, role of users and access rights; • Identify data transmission channels and potential leakages; • Types of data circulation were determined correctly • Identify data transmission flows and possible information leak channels; • Fill in the threat model template;	

	• Prepare report on the audit results, including data flows, potential leakage channels, levels of risks for users roles, security objects (with reference to the regulatory framework and impact assessment methods), user roles, etc.; • Compile the list of legal acts of the Russian Federation applied within the threat model; • Develop a list, description and templates of legal and regulatory documents of the entity ensuring legal use of corporate protection against internal threats to the information security;	
3.	**Development of security policies within the system of corporate protection of information against internal threats**	**3**
	• Develop new and/or modify existing security policies that cut off the data transfer channels and probable incidents as per the Test Project;	
	• Develop or/and modify the security objects, categories, protection technologies in DLP system, etc.	
	• Enter the information security policies in DLP system.	
	• Modify the security policies in IWTM system according to the interception data obtained in practice.	
	• Apply the policies for the traffic control, identification and/or security incidents created by the external threats generator. Maximize a number of security incidents identified.	
	• Work with the interface of the system of corporate protection against internal threats to the information security;	

4.	**Search and prevention of incidents. Technologies of network traffic analysis in the system of corporate protection of information against internal threats**	**3**
	• Develop and apply the policies using regular expressions and morphological search to identify relevant incidents	
	• Develop and apply the policies using search by stamps and letterheads to identify relevant incidents	
	• Develop and apply the policies using search of graphic objects to identify relevant incidents	
	• Develop and apply the policies using search by database to identify relevant incidents	
	• Develop and apply the policies using text recognition mechanisms to identify relevant incidents	
	• Develop and apply the policies working with specific types of files to identify relevant incidents	
	• Identify most of the security incidents in a limited time	
5	**Agent monitoring techniques**	**2**
	• Demonstrate the knowledge of the agent monitoring mechanisms operation	
	• Develop and apply the agent monitoring policies to work with media and devices	
	• Develop and apply the agent monitoring policies to work with files	
	• Working with interception exceptions	
6	**Identified incident analysis**	**2**
	• Preparation of the report on incidents;	
	• Application of mechanisms for creating filters for analyzing intercepted traffic and identified incidents;	
	• Classification of threats by the level of incident threat; Damage evaluation;	

	• Use of additional modules for analyzing information flows, if this is dictated by the specific of doing business;	
	• Development of a plan for further investigation of detected incidents and counteraction with intruders based on the regulatory framework;	
Total		**20 hours**

Depending on the type of competition, the number of modules and implementation time may vary.

3.3. Test Project development

Text documents should be provided in Word format, graphic ones in PDF format.

3.3.1. Who develops Test Project/Module assignments

The Chief Expert with the expert community and the technical experts of the industrial partners companies develop the main assignment modules.

3.3.2. How and when the Test Project/Modules are developed

The experts of the industrial partner of the skill and other experts develop the entity's model (including documents describing the organizational structure) and collect a stand simulating corporate document flow (both legal and illegal security incidents, leaks, etc.). Incidents and data leakage channels are selected in such a way that participants can demonstrate their skills in their detection and prevention.

Additionally, test programs are prepared, which will be used by competitors according assignment.

Experts, participating in the competition for the first time, need to contact the main expert at least 3 months prior to the start date of the competition to discuss the modules that should be used in the competition.

3.3.3. When the Test Project is developed

The Test Project assignments shall be developed before the competition and announced at the current competition.

3 months prior the competition: types of the software applied are announced

1 month prior to the competition: access to the documentation for all components is provided

3.4. The Competition Marking Scheme

The proposed Competition Marking Scheme is developed by the persons developing the Test Project assignment. Final detailed option of the Competition Marking Scheme is developed and approved by all experts, participating in the competition.

3.5. The Competition Assignment selection

Model, legend and description of the production,as well as the scenarios of data leakages are selected by the authorized persons and specialists from the industrial partners' companies.

3.6. Test Project assignment disclosure

Test Project assignment is published on the web-site: www.worldskills.ru **1 month prior** to the current competition.

It is published after the its approval by the authorized persons and specialists from the industrial partners' companies.

3.7. Assignment approval (preparation for competition)

Procedure of the Test Project assignment approval is executed by the Chief Expert and its Deputy

3.8. Possible change of the Test Project assignment

Each Test Project is subject to the 30% change described in the Memorandum of Understanding.

4. SKILL MANAGEMENT AND COMMUNICATION

4.1. Discussion forum

Prior to the competition all discussions, communication, collaboration and decision-making regarding the skill competition shall take place on the skill-specific discussion forum (http://forum.worldskills.ru). The forum moderator is the Chief Expert (or Expert appointed to this position by the Chief Expert). The time-frame for exchange of messages and the requirements to development of the competition are set by the Competition Rules.

4.2. Information for competitors

All information for registered competitors is available at the Centre for competitors (http://www.worldskills.ru).

This information includes:

- Rules (Regulations) of the Competition
- Technical Descriptions
- Competition Assignments
- Other information relating to the competition.

4.3. Competition Assignments

Announced Test Projects can be found at the website forum.worldskills.ru

4.4. Current management

Existing management is defined in skill competition plan, which is developed by the Skill Management Group headed by the Chief Expert, at the competition venue. The Skill Management Group consists of the Jury President, Chief Expert, and Deputy Chief Expert. The skill competition plan shall be developed six months prior to the competition and shall be finalized during the competition by a joint decision of the Experts. Skill competition plan can be found at the website www.worldskills.ru.

5. ASSESSMENT

Test Project/Module assessment by the WSR Experts is described in this section. The scores characteristics and scoring procedures and requirements are specified here as well.

5.1. Assessment criteria

This section defines the assessment criteria and the number of marks (subjective and objective) given. The total number of marks for all assessment criteria is 100.

Section	Criterion	Points	
		Objective	Total
A	Work organization and management	6.50	6.50

B	Determination, configuration and elimination of faults in the system of corporate protection against internal threats	14.00	14.00
C	Examination (audit) of the entity for internal threat protection	10.00	10.00
D	Development of security policies within the system of corporate protection of information against internal threats	16.50	16.50
E	Search and prevention of incidents. Technologies of network traffic analysis in the system of corporate protection of information against internal threats	37.00	37.00
F	Agent monitoring techniques	9.00	9.00
G	Identified incident analysis	7.00	7.00
Total =		**100**	**100**

5.2. Subjective marks and Judgment marks

Not applicable.

5.3. Skills Assessment Criteria

Professional skills are assessed by multiple categories with the assistance of the industrial specialists on this skill.

Final assessment criteria shall be approved by the specialists from the industrial partner company.

Test Project implementation time is a criteria for assessment of individual skills.

5.4. Standing orders for skill assessment

- The Chief Expert divides the Experts into groups (depending on the number of experts), so that in each group there are both experienced participants of the WorldSkills events and newcomers.
- One group of the experts assigned by the Chief expert or his Deputy shall measure the objective parameters of the Test Project.
- Another group shall be at the competition site and follows the competitor's performance.
- At the end of each day, the measurement results are signed individually by each expert responsible for the competitor and marks are entered in the CIS.
- There are no special standing orders for marking.

7. BRANCH OHSE REQUIREMENTS

See the OHSE documentation of the competition host country.

Being on the work site, all competitors are obliged to observe the safety rules when working on a computer.

7. MATERIAL AND EQUIPMENT

7.1. Infrastructure list

All equipment, materials, and devices provided on site are listed in the Infrastructure List.

The Infrastructure List is available on web-site: http://www.worldskills.ru

The Competition Organizer shall update the Infrastructure List specifying the necessary quantity, type, brand/model of items.

During each Competition, the Experts study and specify the Infrastructure List for the preparation to the next Competition. The Experts provide the Technical Director with the recommendations on the premises expansion and equipment list change.

During each Competition, the WSR Technical Director checks the Infrastructure List used at the previous Competition.

The Infrastructure list does not contain items that competitors and/or Experts bring and items that competitor's are not allowed to bring. These items are listed below.

7.2. Materials, equipment and tools supplied by competitors in their toolbox

Equipment/materials of the competitors shall not be used in the skill. Toolbox is not available.

7.3. Materials, equipment and tools provided by Experts

Not used.

7.4. Materials and equipment prohibited on site

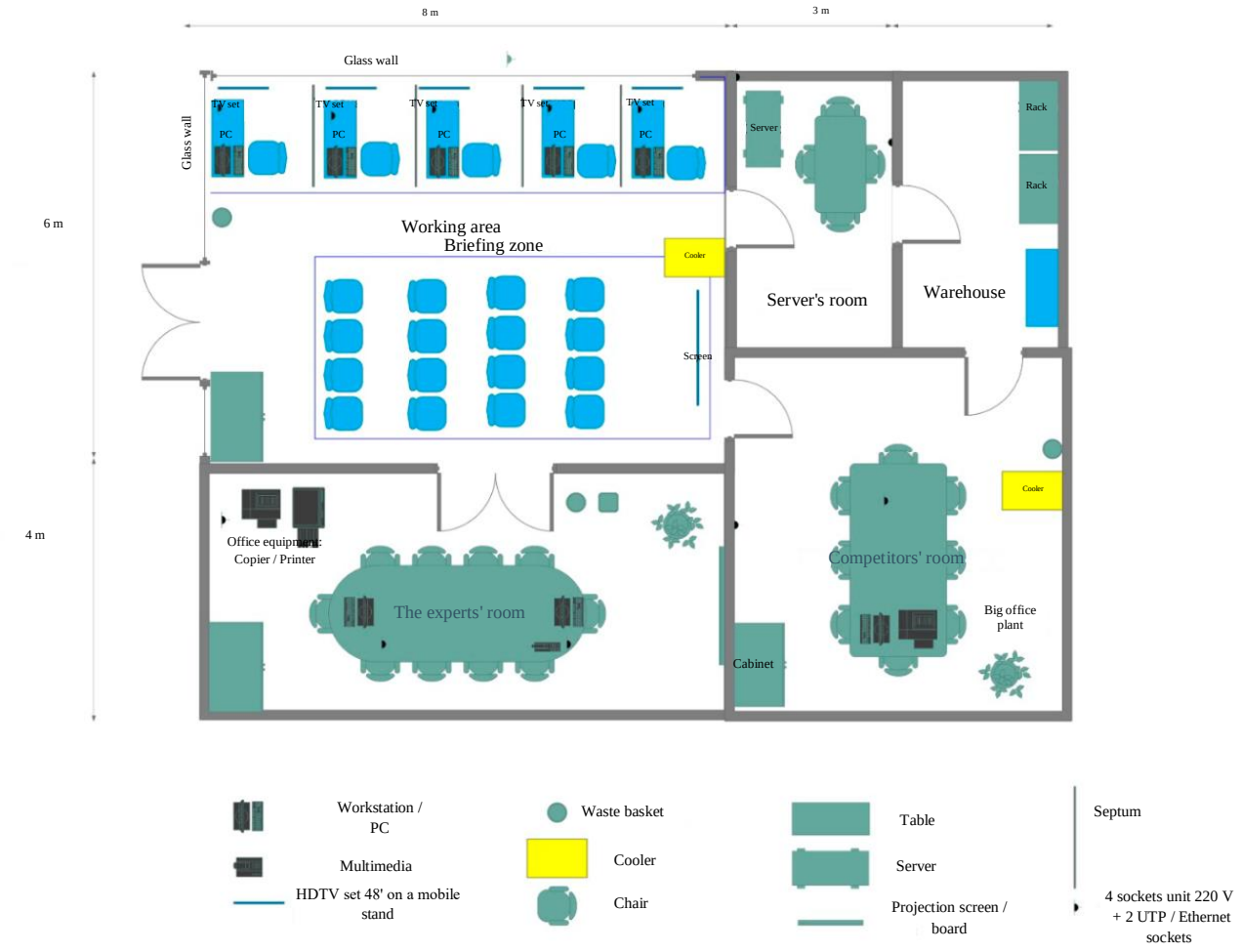
The materials and equipment listed in Item 7.2 are allowed

7.5. Proposed layout of the work place

The layouts can be found at the web-site: www.worldskill.ru

Workshop scheme

(*please, see Picture 1*)



8. PRESENTATION OF THE SKILL TO THE VISITORS AND MEDIA

8.1. Maximum engagement of visitors and media

Below is a list of all possible methods of visitors and media engagement in the process of a body repair process.

- The screens streaming the competition process to the WorldSkills website
- Description of tests (available to viewers)
- Interactive zones
- Providing the viewers with the detailed description of the competitors' activity
- Curriculum vitae and national flags of the competitors
- Master classes
- Understanding of what the competitors are doing;
- Information on competitors (competitors profiles);
- Creer prospects;
- Daily media coverage of competition.

8.2. Rules for the visitors and guests

Visitors and guests have access to the competition site only with the permission of the Chief Expert.

8.3 Rules for media

- Representatives of accredited media have access to the competition site only with the permission of the Chief Expert,
- Making photos and videos by the audience is permitted.

9. SPECIAL RULES FOR THE 14–16 AGE GROUP

The Test Project performance time shall not exceed 4 hours per day.

During the development of the Test Project and the Marking Scheme, it is required to consider the specific features and the limitations of the applied OHSE rules for this age group. It is also required to take into account anthropometric, psychophysiologic and psychological characteristics of this age group. This way, the Test Project and the Marking Scheme can cover not all of the WSSS units and areas depending on the specific features of the skill.