Access and Security Agreement

-

Standard

Version 1.0

Version Control

Scope
This document is the standard security agreement for all situations where third party staff is given access to Shell IT infrastructure, but no Access and Security Appendix has been attached to the business agreement with that third party.

Owner
de Boer, Jeroen SI-ITC/R

Author

Matthijs Nieuwveld – Legal Counsel

Version History

Number	Revision Date (dd/mm/yyyy)	Contributor's Name	Revision Description
1.0	19/04/2013	Matthijs Nieuwveld, Jeroen de Boer	Approved Version

Drafting Notes
Parts in BLUE only to be used if or to the extent applicable. Please review and DELETE footnotes & instructions and amend as instructed prior to sending the template to a third party.

THIS ACCESS AND SECURITY AGREEMENT is made between

1. **[FULL NAME OF THE SHELL ENTITY]**, [a limited liability company incorporated under the laws of the Netherlands, having its registered office at Carel van Bylandtlaan 30, the Hague, the Netherlands] / [a company incorporated under the laws of […] and having its registered office at […]] ("**Shell**");

and

2. **[FULL NAME OF THE CONTRACTOR ENTITY]**, a company incorporated under the laws of […] and having its registered office at […] ("**Contractor**");

hereinafter individually also referred to as "**Party**" and collectively as "**Parties**".

WHEREAS:

A. Shell and Contractor entered into a certain agreement pursuant to which Contractor performs certain works and/or services for Shell;

B. In order to provide those certain works and/or services Contractor needs access to certain Shell IT Infrastructure; and

C. Parties wish to lay down the rights and obligations concerning the access to Shell IT Infrastructure in this Agreement.

THE PARTIES HEREBY AGREE as follows:

ARTICLE 1. - DEFINITIONS

1.1. Capitalised terms used in this Agreement shall have the meaning ascribed to them below:

"Affiliate of Shell"	means (a) any person that directly or indirectly controls or is controlled by Shell; or (ii) is directly or indirectly controlled by a Person that also directly or indirectly controls Shell and/or (b) any Person in which Shell, or a Person under (a) above, holds, whether directly or indirectly, any participating interest, equity, shares or voting rights. For the purpose of this definition a Person controls another Person if such Person (i) holds fifty percent (50%) or more of the participating interest, equity, shares or voting

	rights in such Person, or (ii) has the power to direct or cause the direction of the management and policies of the other Person, whether directly or indirectly, through one or more intermediaries or otherwise, and whether by ownership of shares or other equity interests, the holding of voting rights or contractual rights, by being the general partner of a limited partnership, or otherwise.
"Agreement"	means this Access and Security Agreement.
Applicable Law	means in relation to a Person, property or circumstance, statutes (including regulations enacted thereunder); judgments and orders of courts of competent jurisdiction; rules, regulations and orders issued by government agencies, authorities and other regulatory bodies; and regulatory approvals, permits, licenses, approvals and authorizations; that are applicable to such Person, property or circumstance.
"Authorized Users"	means the Contractor Personnel, approved in accordance with Article 5, who may access the Shell IT Facilities and/or the Shell IT Equipment and **Authorized User** means any one of them.
"Client Software"	has the meaning ascribed to it in Article 11.1.
"Contractor Personnel"	means any individual assigned or used by Contractor, whether directly or indirectly, to work in connection with the execution of the Original Agreement, whether or not an employee of Contractor.
"Means of Identification and Authentication"	means the means provided by Shell to Contractor and/or Authorized Users used to identify and authenticate such Authorized Users, such as, but not limited to, a user-id and password or a smart card and pin.
"Person"	means any individual, partnership, limited partnership, firm, trust, body corporate, government, governmental body, agency or instrumentality, or unincorporated venture.
"Security Incident"	means a successful or unsuccessful attempt to

	access, use, steal, disclose, modify or destroy information and interference with or misuse of information process infrastructure, applications and data.
"Security Standard"	means information security specifications, standards and practices that are generally recognized as being sufficient to safeguard IT equipment, such as the ISO 27001/2 standard, as amended from time to time, which will – at a minimum – include: (i) running a fully patched version of the operating system for which the vendor actively provides security patches; (ii) running up to date anti-Virus software; (iii) running an up to date personal firewall; (iv) systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts; (v) design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and (vi) adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.
"Shell Data"	means any data obtained (i) from Shell, (ii) from an Affiliate of Shell, or (iii) via the Shell IT Equipment or Shell IT Facilities.
"Shell IT Equipment"	means those items of equipment, machinery components, instruments and accessories, together with any documentation being provided by Shell, and/or Affiliates of Shell.
"Shell IT Facilities"	means those applications, services, network connections, communications together with any documentation and any other facilities being provided by Shell and/or Affiliates of Shell.
"Shell IT Infrastructure"	means the Shell IT Equipment, the Shell IT Facilities and/or the Shell Data.

ARTICLE 2. – TERMINATION RIGHT

Any material breach of the terms of this Agreement shall give Shell the right to immediately terminate this Agreement and any access provided to the Contractor and/or the Authorized Users, even if that access is provided under another arrangement.

ARTICLE 3. – SECURITY STANDARDS

3.1. IT equipment used to (i) connect to Shell IT Equipment and/or Shell IT Facilities, and/or (ii) process and store Shell Data, must be managed in compliance with the Security Standard.

3.2. Shell can impose additional security standards and/or controls on IT equipment used to (i) connect to Shell IT Equipment and/or Shell IT Facilities, and/or (ii) process and store Shell Data by so notifying the Contractor. Contractor shall implement such additional security standards and/or controls within 14 days of notification.

3.3. Contractor shall maintain clear guidelines and policies for disciplinary action associated with breach of the Security Standard or other security policies and shall operate an effective security education program for their staff on a continuous basis.

3.4. Contractor shall notify Shell of any material changes to the Contractor's Security Standards, information security strategy, policies, operational standards or procedures.

ARTICLE 4. – CONTRACTOR'S OBLIGATION

4.1. Contractor shall (i) access the Shell IT Infrastructure solely for the execution of the work for which Contractor is engaged by Shell, (ii) not attempt to (a) access any other systems, (b) modify or add to the Shell IT Facilities and/or Shell IT Equipment, (c) attempt in any way to disable or reconfigure any log files or facilities on Shell IT Equipment and/or Shell IT Facilities, or (d) install or cause to be installed into or on Shell IT Equipment and/or Shell IT Facilities any hardware, software, electronic, or other security mechanism or other disablement, deactivation, deinstallation, damage or deletion mechanism which will hinder use of any of the Shell IT Infrastructure, or (iii) use the access to the Shell IT Infrastructure for any other purpose inconsistent with the spirit of this Agreement.

4.2. Contractor shall ensure that Shell Data is at all times segregated from the data of third parties and Shell Data classified as '*Most Confidential*' shall not be accessed or stored.

ARTICLE 5. – ACCESS FOR AUTHORIZED USERS

5.1. Contractor shall not allow access to Shell IT Infrastructure to others than the Authorized Users and concurs that Authorized Users email addresses may be added to the Shell global address list.

5.2. Contractor may nominate only Contractor Personnel as Authorized Users. Contractor may nominate additional Authorized Users by submitting their name and location of use to Shell. Shell may accept or reject a nomination for an additional Authorized User at its sole discretion.

5.3. Upon completion of any required training and instructions the Authorized Users shall be issued a Means of Identification and Authentication. Contractor shall maintain an up-to-date list of the Authorized Users who have been given a Means of Identification and Authentication and shall notify Shell as soon as possible of any Authorized Users who's access can be terminated.

5.4. Authorized Users shall be given access to those parts of the Shell IT Equipment and/or Shell IT Facilities as is reasonably required for the execution of the work for which Contractor is engaged by Shell.

5.5. Authorized Users shall be required to accept terms of use before they can access certain Shell IT Infrastructure. Contractor hereby gives the Authorized Users permission to also accept the relevant terms of use on its behalf and Contractor warrants that the Authorized Users shall adhere to the terms of this Agreement and the terms of use.

5.6. Prior to the issue of a Means of Identification and Authentication, Contractor shall provide the Authorized Users with all instructions as requested by Shell.

5.7. In the event that the Means of Identification and Authentication is issued in the form of a smart card or a user-id and password, Contractor shall instruct Authorized Users to:

(a) not disclose or give their smart card, user-id or password to any other person (including any other Authorized User) nor write down their user-id or password;
(b) not store their user-id or password in any data file, unless such file is encrypted;
(c) refrain from any action that could allow any person to gain access to their smart card, user-id or password;
(d) make every reasonable effort to prevent any situation that would allow any person to obtain access to their smart card, user-id or password; and
(e) adhere to any other instructions that may be provided by Shell.

ARTICLE 6. – CONFIDENTIALITY

6.1. Contractor shall, and shall procure that the Authorized Users shall, maintain in confidence and not disclose to any third party all Shell Data, unless (i) disclosure is necessary for the performance of the work for which Contractor is engaged by Shell, provided that the receiving party has agreed to be bound by confidentiality provisions no less stringent than those assumed by the Contractor hereunder or (ii) required by law.

6.2. At Shell's request, Contractor shall promptly return any and all Shell Data, together with any copies or extracts thereof, as so requested by Shell at any time and to destroy all analyses, compilations, studies or other documents, hard or electronic, that reflect any Shell Data.

6.3. Contractor acknowledges and agrees that any Shell Data received by it and/or an Authorized User is on an "as is" basis, and Shell makes no representation or warranty as to the accuracy of the Shell Data or as to its satisfactory quality, fitness or suitability for a particular purpose.

ARTICLE 7. – MAINTENANCE AND SUPPORT

Shell IT Equipment and Shell IT Facilities are maintained, and may be located, by Shell and/or third party suppliers engaged by Shell. Support to Contractor and/or Authorized Users by Shell is limited to access technology only and shall be provided in English.

ARTICLE 8. – INDEMNITY AND WARRANTY

8.1. The Contractor's and Authorized Users' access to and use of the Shell IT Infrastructure is at the Contractor's own risk. The Contractor shall indemnify and hold Shell, or any Affiliate of Shell, harmless from any claim by Authorized Users or third parties.

8.2. Shell makes no representations, extends no warranties of any kind, either express or implied, accepts no liability, and assumes no responsibilities whatsoever with respect to fitness for a particular purpose, merchantability, non-infringement, suitability, accuracy and/or completeness of the Shell IT Infrastructure and/or any software provided by Shell, all to the fullest extent permitted by law.

8.3. Shell extends no warranty concerning the results or effects of the use of the Shell IT Infrastructure and does not guarantee that the access to the Shell IT Infrastructure will not be interrupted or error free.

ARTICLE 9. – AUDIT RIGHT

9.1. Shell reserves the right to log and monitor the use of any Shell IT Infrastructure at any time without notice. Such monitoring may include inspection of the Shell IT Infrastructure.

9.2. The Contractor shall permit Shell or its authorized representatives, at all reasonable times, to audit the Contractor's and the Authorized User's (i) compliance with this Agreement and (ii) use of the Shell IT Infrastructure, together with other records, correspondence or other papers and data carriers in possession of Contractor and/or Authorized Users that are necessary for Shell to carry out such audit.

9.3. Shell or its duly authorized representatives shall have access to all Contractor Personnel and to any and all material related to this Agreement. Contractor shall maintain such material for a minimum period of four (4) years, or the length of time required under the Applicable Law, which ever is longer, from the termination of this Agreement. Shell or its duly authorized representatives shall have the rights to reproduce and retain copies if the aforementioned material.

9.4. The audit may take place under the supervision of a Contractor representative at Contractor's place of business.

ARTICLE 10. – SECURITY INCIDENT MANAGEMENT PROCEDURES

10.1. Contractor shall, and shall procure that the Authorized Users shall, report to Shell in a readily-accessible format and without delay all (i) Security Incidents, (ii) suspected Security Incidents, (iii) near-misses, (iv) suspected near misses, (v) anomalies, (vi) contact by law enforcement, (vii) regulatory or security authorities, and (viii) civil injunctions or search orders, all in as far as they impact, or might impact, Shell IT Infrastructure.

10.2. Contractor shall, and shall procure that the Authorized Users shall, cooperate with investigations deemed necessary by Shell in the event of a (suspected) Security Incident. In the event of a (suspected) Security Incident, Contractor shall reasonably collaborate with Shell in the root cause analysis and the forensic investigation of the (suspected) Security Incident.

10.3. Contractor shall, and shall procure that Authorized Users shall, ensure that in the event of a security incident the overall business impact for Shell shall be minimized and all Shell Data shall be isolated in such a way as to minimise loss or damage to Shell IT Infrastructure.

10.4. Contractor shall comply with (i) the "*Shell Investigation Principles*" document, as attached as **Schedule I**, (ii) the "*Code of Conduct*" document, as attached as **Schedule II**, and (iii) the "*Shell General Business Principles*" document, as attached as **Schedule III**.

ARTICLE 11. – CLIENT SOFTWARE

11.1. Shell may make available client software for use on Authorized Users computer in order to provide the necessary access to Shell IT Equipment and/or Shell IT Facilities (the "**Client Software**").

11.2. The intellectual property rights of the Client Software shall not transfer to Contractor or the Authorized Users but will remain with the owner thereof. Shell assumes responsibility for Authorized Users' use of the Client Software in accordance with this Agreement, including, for clarity purposes, any (alleged) third party infringements claims made against Contractor or Authorized Users in respect of such use.

11.3. Contractor shall, and shall procure that the Authorized Users shall, ensure that the Client Software shall only be used for the execution of the Agreement and shall not be distributed, copied, reproduced, translated, adapted, modified or reverse engineered.

ARTICLE 12. – EXPORT CONTROLS AND ENCRYPTION

12.1. The Client Software may be of 'U.S. origin' and may be subject to special restrictions, including limitations on who can download the Client Software and where it can be used. Shell shall provide relevant export control details upon specific request by the Contractor and/or a Authorized User.

12.2. Contractor shall, and shall procure that the Authorized Users shall, comply with all relevant export control regulations and all Aplicable Law. Client Software of U.S. origin may not be used in a U.S. Generally Embargoed Country or a Highly Restricted country, nor can it be used by nationals of any of these countries. The list of countries and regulations thereof are subject to change, and Contractor shall ensure to be up-to-date and aware of any changes to these regulations.

12.3. The Client Software may contain encryption functionality. Various countries have laws on importing and using encryption functionality. Contractor shall ensure (i) compliance with those laws and (ii) that all Authorized Users shall check whether they are allowed to bring encryption functionality into their destination country before travelling with and/or downloading the Client Software.

12.4. Contractor or Authorized Users shall not provide any encryption keys to any authorities without first receiving approval from Shell. If such is not possible, Contractor shall inform Shell of the provision of encryption keys as soon as possible.

ARTICLE 13. – TERMINATION OF SERVICE

13.1. Shell may, at any time, terminate the access to Shell IT Equipment and/or Shell IT Facilities for one or more Authorized Users.

13.2. Upon termination of access, Contractor shall make sure that all Client Software is removed from the relevant IT equipment and all relevant Means of Identification and Authentication are returned to Shell as soon as possible.

13.3. Upon termination of the Agreement, Contractor shall immediately stop any access by the Authorized Users to the Shell IT Infrastructure, and shall ensure that all Shell IT Infratructure, software and/or any other materials provided under this Agreement, including all copies and documentation, whether contained on media or data carriers or not, relating thereto are returned to Shell or, if so directed by Shell, destroyed as soon as possible.

13.4. The termination of this Agreement shall not prejudice any rights or remedies accruing to Shell or the Contractor before such termination took effect or relieve either party of any continuing obligations under this Agreement or at law.

ARTICLE 14. - GOVERNING LAW AND ARBITRATION

14.1. This Agreement shall be governed by and construed in accordance with the laws of the Netherlands.

14.2. Any dispute arising out of, or in connection with, this Agreement ("**Dispute**") shall be amicably settled by the Parties.

14.3. If the parties are unable to amicably settle a Dispute within 60 days, such Dispute shall be settled by the courts of The Hague, the Netherlands.

-- Signature page follows -

THUS AGREED BY THE PARTIES ON […]

_____	_____
[Shell Entity]	**[Shell Entity]**
Name: Title:	Name: Title:
_____	_____
[Contractor Entity]	**[Contractor Entity]**
Name: Title:	Name: Title:

SCHEDULE I – SHELL INVESTIGATION PRINCIPLES

Adobe Acrobat Document

Please print and attach the below Adobe Document. The latest version can also be downloaded from: http://sww.shell.com/audit/business_integrity_department/H8882_SIA_IP_Leaflet_5_HR1.pdf

SCHEDULE II – CODE OF CONDUCT

Please print and attach the below Adobe Document. The latest version can also be downloaded from: http://www.shell.com/home/content/aboutshell/who_we_are/our_values/code_of_conduct/

CODE OF CONDUCT

Helping you live by our Core Values and our General Business Principles

SCHEDULE III –SHELL GENERAL BUSINESS PRINCIPLES

Please print and attach the below Adobe Document. The latest version can be downloaded from: http://www.shell.com/global/aboutshell/who-we-are/our-values/sgbp.html

SHELL GENERAL BUSINESS PRINCIPLES