Horsham District Council

Information Security Policy Suite

Access Control Guidelines

including

Supplier Access

Contents

1. Supplier Access

This section provides guidelines for third-party suppliers to enable them to install and support software packages on the Council's computer systems. The key objective is to protect the Council's systems from accidental or malicious damage.

1.1 Pre-requisites

a. Before being given access to Council systems for software installation or configuration changes, suppliers must undertake to protect the Council's information and sign the Council's Data Protection Statement (see Appendix 1 on page 6) OR have a suitable Confidentiality Agreement in place (this may form part of an existing support contract).

b. Suppliers should ensure that their staff are adequately trained to perform any work on the Council's systems and that they exercise care in the performance of that work to prevent damage to those systems.

c. When given access to the Council's systems, suppliers must not create login accounts or any other means of accessing those systems other than those supplied by the Council's. Suppliers must not access systems other than those to which they have been granted access.

1.2 Software

1.2.1 Installations and Upgrades

1.2.1.1 Pre-install

a. Before installing software or making configuration changes to any the Council's systems, suppliers must discuss with the System Administrator and / or Technology Services exactly what they intend to do.

b. The work to be done needs to be agreed before any work commences.

c. Suppliers should indicate whether it must be necessary to reboot a server.

d. Some installation must be carried out on live servers or those that are in use by technical or development staff and these should not be rebooted without prior agreement with the Technology Services Help Desk who will give advance notification to end users.

e. Suppliers should not make any other changes without further discussion and agreement with the Systems Administrator and / or Technology Services.

f. If problems are encountered which necessitate changes to the agreed plan the changes should be discussed and agreed.

1.2.1.2 During Installation

g. Where installation requires Administrator access this should only be provided as a local privilege and use should be closely monitored by the System Administrator.

h. A new local Administrator account must be created by the Council's for this purpose. This account must be disabled immediately after installation is complete.

i. Domain Administrator rights will never be given to third parties.

1.2.1.3 Changes to System Components

j. Suppliers should not make changes to standard system components, e.g. installing later versions of software such as Internet Explorer, installing Service Packs without express permission from a member of the Technology Services Management team.

k. If such changes are deemed necessary, they should be notified before the installation visit so that the impact of the changes can be assessed by Technology Services.

l. Reasons for the change should be given along with a statement of the impact if it is decided that the changes are unacceptable.

1.2.1.4 Distribution

m. Suppliers are expected to assist Technology Services in the creation of automatic software distribution packages which can be automatically delivered to client PCs through the use of Group Policies.

1.2.2 Remote Access for Support Purposes

n. Administrator rights will not be allowed for remote access accounts. Where this is considered to be a problem the supplier should discuss with Technology Services what additional permissions and rights need to be applied without giving full Administrator privilege.

o. Where remote access is needed this must be provided through the Council's Remote Access solution, e.g. Supplier Gateway.

p. Use of approved third party remote support solutions is permitted, e.g. GoToAssist, Netviewer, etc.

q. Suppliers may use the Microsoft Terminal Services Client to gain access to necessary servers by prior agreement with the technology Services Management Team.

r. Configuration details for the connection must be supplied by Technology Services.

1.3 Disclosure of Information

a. Any data or information that is obtained by suppliers, whilst on-site or connected to the Council's Data Network, remains the property of the Council and should be returned or destroyed in such a way as to be un-recoverable by unauthorised person(s) unless otherwise agreed by the Data Protection Officer in compliance with any relevant legislation.

b. Suppliers will agree that they will not directly or indirectly use, divulge, disclose or communicate to any person, firm or corporation any Confidential and Proprietary Information, unless it is with the written permission of the Data Protection Officer of the Council.

c. Any connection to the Council's Data Network may not be used in any way that violates the Council's Information Security policies, standards, guidelines or procedures.

d. Any connection to any part of the Council's Data Network may not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes and deliberate tampering (e.g. spreading computer viruses).

1.4 Legal requirements

Suppliers must be aware of and comply with relevant legislation whilst connected to the Councils Data Network or when handling Council data, e.g.

a. Computer Misuse Act 1990
b. Data Protection Act 2018
c. Freedom of Information Act 2000
d. Human Rights Act 1998
e. Protection of Freedoms Act 2012
f. Regulation of Investigatory Powers Act 2000

Appendix 1: Supplier's Data Protection Declaration

The Supplier detailed below is to be allowed access to {insert name of Council} Council computer systems (either directly or remotely) for the purpose of installation and support of a software package. The facility will necessitate **The Supplier** having access to personal and confidential information on the System, and the Council needs to be satisfied as to the confidentiality and security of this information.

In connection with the Facility, the Council will authorise **The Supplier** to have access to any data on the System (including any personal data as defined in the Data Protection Act 1998) only to the extent necessary and solely for the purpose of enabling it to carry out its obligations under the Facility including, without limitation, those cases where **The Supplier** is resolving a support or maintenance problem, or testing a new system for the Council.

The Supplier is asked, therefore, to give the following undertakings to the Council, the intention being that the undertakings shall continue without limit in point of time but shall cease to apply to any information coming into the public domain otherwise than by a breach of the undertakings by **The Supplier**.

1. That any copy data created must be destroyed immediately after it has been used;

2. That it will keep confidential (and procure that its employees and agents shall keep confidential) any confidential information which it or they may acquire in the course of providing to the Council the Facility in respect of the System, and shall not use or disclose such information except in accordance with the Order of a Court of competent jurisdiction; and

3. That it shall use its best endeavours to ensure that its officers, employees and agents observe a similar obligation of confidence.

It is to be understood that these undertakings given by **The Supplier** in favour of the Council shall not prevent **The Supplier** from disclosing any such information to the extent required in or in connection with legal proceedings arising out of its providing the Facility to the Council.

If **The Supplier** is prepared to give these undertakings, please indicate this by signing and returning the duplicate of this document to Horsham District Council Technology Services Team c/o {insert name of Council and full mailing address here}. Alternatively, do you wish to have these undertakings embodied in a formal Confidentiality Agreement?

I agree to the terms outlined in this document.

Company Name: _____

Print Name: _____

Signed: _____ Date: / /