Delphi Information 3rd Party Security Requirements Summary

Classified: Public

5/17/2012

Contents

Introduction 3

Summary for All Users 4

Vendor Assessment Considerations 7

Introduction

Delphi security policies cover the management of security for both Delphi internal operations as well as the services Delphi provides to its customers. The Delphi Information Security policy applies to all Delphi employees. The policies are confidential information and are not available for review by Customer or third parties. However, brief summaries of certain Delphi security policies relevant to the engagement of Third Party Service Providers are provided below.

This document summarizes the security policies and practices required by Delphi from Third Party companies providing services that include:

- The creation of, purchase of, or right to use software, web application, IT utilities, and/or hardware

OR

- the capture, storage, or transfer of Delphi data, whether standalone by the supplier, between Delphi and the supplier, or between third parties

Lack of inclusion or omission of a particular subject in this summary does not eliminate oversight and responsibility on behalf of the Third Party, and they are expected to exercise due care and sound judgment, and recognize potential Information Security concerns or risks.

Delphi expects evidence ensuring these policies and requirements are met will be provided upon request

Any awareness of an information security concern, or any doubt or question with respect to information security guidance or practices, should be immediately directed to the Delphi Information Security Team at informationsecurity@delphi.com .

Summary for All Users

Delphi computing and data communications are valuable and limited resources that serve a large number and variety of users. (NOTE: A “user” is any Delphi person, including: permanent/full-time employees, temporary employees, contractors, and any other individual that is working with or on behalf of Delphi, and/or has access to Delphi information or resources.)

All users have the responsibility to make use of these resources in an efficient, ethical, and legal manner.

These policies apply to all users of Delphi information globally, including visitors, contractors, suppliers and employees. These policies also apply to all information systems owned, contracted, leased or operated for or by Delphi, connected to the Delphi network, or used to process, stored or transfer Delphi data.

Delphi reserves the right to scan and monitor system access and use.

Delphi’s computer and network services provide access to resources both within and outside the Delphi environment. These services must be used in a manner consistent with the mission and objectives of Delphi and with the purpose for which such use was intended.

Such open access is a privilege, and imposes upon users certain responsibilities and obligations. Access to Delphi's computers and network services is granted subject to Delphi policies, and applicable laws.

Acceptable use is always ethical, reflects professional integrity, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, protection of sensitive information, ownership of data, copyright laws, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation and harassment.

All activities inconsistent with these objectives are considered to be inappropriate and may jeopardize continued use of computing facilities and networks.

In consideration of being allowed to use the Delphi computer and network services ("Resources"), all users must understand and agree to the following:

1. Users shall not use the Resources for any illegal activity or for any activity prohibited by this policy (see subsequent examples of inappropriate conduct that is prohibited).

2. Users agree not to use the Resources to infringe upon or otherwise impair, interfere with or violate any copyright or other intellectual property rights of another. This pertains to all

Delphi intellectual property as well as copyrighted material, including, but not limited to music, video and software.

3. Users shall avoid any action that interferes with the efficient operation of the Resources or impedes the flow of information necessary for conduct of Delphi business.

4. Users shall protect their computer resources such as ID, logins and systems from unauthorized use. Users are responsible for reasonably securing their computer, including implementing such protections as logins to prohibit unauthorized use.

5. Users will access only information that is their own, or to which their access has been authorized. Users will only access networks, network resources, and information for their intended use.

Examples of Inappropriate Use of Resources include, but are not limited to:

- Accessing another person's computer, computer account, files, or data without permission.

- Using the Delphi network to gain unauthorized access to any computer system.

- Using any means to decode or otherwise obtain restricted passwords or access control information.

- Attempting to circumvent or subvert system or network security measures. Examples include creating or running programs that are designed to identify security loopholes, to decrypt intentionally secured data, or to gain unauthorized access to any system.

- Engaging in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files or making unauthorized modifications to Delphi data.

- Performing any act, intentionally or otherwise, that will interfere with the normal operation of computers, peripherals, or networks.

- Making or using illegal copies of copyrighted software, storing such copies on Delphi systems, or transmitting them over Delphi networks.

- Harassing or intimidating others via electronic mail, news groups or Web pages.

- Initiating or propagating electronic chain letters.

- Initiating or facilitating in any way mass unsolicited and unofficial electronic mailing (e.g., "spamming", "flooding", or "bombing.").

- Forging the identity of a user or machine in an electronic communication.

- Saturating network or computer resources to the exclusion of another's use, for example, overloading the network with traffic such as emails, excessive file backup/archive, or malicious (denial of service attack) activities.

- Using Delphi systems or networks for personal gain; for example, by selling access to your ID or to Delphi systems or networks, or by performing work for profit with Delphi resources in a manner not authorized.

- Engaging in any other activity that does not comply with the general principles presented above.

Vendor Assessment Considerations

The following list intends to serve as considerations for assessing the risks associated with service providers' information technology practices, processes and controls. It is based on the ISO 27002 framework and presents a list of expectations for each of the ISO domains.

While the specific controls and requirements can vary considerably with the nature or scope of the service, the following serves as a foundation to understand and manage the service providers' risks.

The specific controls and amount of evidence required around those controls can also vary considerably with the nature and scope of the service provided, and will be determined on a case by case basis.

Domain: Security Policy	
Expectations:	All vendors and Service Providers should have and adhere to a written and comprehensive set of information security policy documents, which act as the rules and guidelines for dealing with the protection of information and information assets.
Documents that may be requested:	• Security policy • Procedures and/or standards supporting the policy • Document update schedule • Evidence of policy review • Audit report of security policy
Domain: Organization of Information Security	
Expectations:	A management framework should be established to initiate and control the implementation of information security within the Service Provider's organization. The Service Provider should have a process to review all dependent Service Providers' security policies and procedures to ensure that appropriate security language is incorporated into all third-party agreements.
Documents that may be requested:	• Information security organization chart (including where information security resides in the organization) • Roles and responsibilities • Job descriptions • Overview of access administration process and procedures • Third-party security reviews/assessments • Due diligence performed on third parties
Domain: Asset Management	
Expectations:	Service Providers should have in place an

	appropriate asset control policy structure, including appropriate ownership, management, licensing and other controls that address the following asset types: information assets, software assets, physical assets, and services. The information and materials processed, stored or transmitted by the Service Provider should be handled in accordance with the classification (e.g., confidential, sensitive, public) of the information.
Documents that may be requested:	• Asset control policy • Data classification policy
Domain: Human Resources Security	
Expectations:	Service Providers should have and adhere to policies and procedures in place to perform background checks for those individuals who will be administering systems or have access to Receiver Company information. These policies and procedures should ensure that personnel responsible for design, development, implementation and operation are qualified to fulfill their responsibilities. All employees of the Service Provider's organization, and where relevant, third-party users, should be made aware of information-security threats and concerns, and should be equipped to support the organizational security policy in the course of their normal work.
Documents that may be requested:	• Employment policy • Non-disclosure agreements • Background check documents for staff supporting very sensitive services or data
Domain: Physical and Environmental Security	
Expectations:	Business information processing, storage or distribution facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. Facilities should be physically protected from unauthorized access, damage and interference. Access should be logged and logs should be securely maintained. Equipment should be physically protected from security threats and environmental hazards in order to prevent loss, damage or compromise of assets and interruption to business activities.
Documents that may be requested:	• Floor plan • Badge control policy • Physical access logging policy • Copy of insurance declaration pages
Domain: Communications and Operations Management	
Expectations:	Responsibilities and procedures for the management and operation of all information-

	processing facilities should be established and adhered to. This includes the development of appropriate operating instructions, and change control and incident-response procedures. Segregation of duties and environments—development, testing, staging, and production—should be implemented where appropriate to reduce the risk of negligent, inadvertent or deliberate misuse of information-processing facilities and systems. Controls should be in place to prevent and detect the introduction and dissemination of malicious software. Recovery plans should be prepared, updated and tested regularly. Routine backup procedures should be established and adhered to for carrying out the agreed backup strategy, such as taking backup copies of data, rehearsing their timely restoration, logging events and faults, and, where appropriate, monitoring the equipment environment.
Documents that may be requested:	• Network diagram • Dataflow diagram • SOPs (standard operating procedures) • Desktop procedures • Operations (network, processing) and incident response team organization charts • Office/employee awareness materials and corporate policies • Evidence of frequency of awareness plans • Change control manual • System and network outage and capacity utilization records • Incident-identification and response records • Test plans and results • Third-party due diligence records and contracts • Planning and acceptance records
Domain: Access Control	
Expectations:	Service Providers should have and adhere to a documented policy to ensure that only properly approved users are granted access to systems and assets. Users should be granted access on a need-to-know basis, according to job responsibilities. The access-control policy should employ methods designed to physically and logically restrict access to equipment, ensure the identification and authentication of individuals who access computing resources, and restrict an individual's access to information once the individual has accessed a system. Depending on the level of protection required (based on the asset classification); a combination of access-control techniques may need to be employed. Users should be aware of their responsibilities for maintaining effective access controls, particularly

	as they relate to password security and user equipment. Service Providers should have a written authorized user accountability policy that incorporates authentication standards and clearly articulates user responsibilities.
Documents that may be requested:	• Security policy with access policy • User policy and network access controls • Network architecture diagram (including placement of firewalls) • Application access control procedures • Dataflow diagram
Domain: Information Systems Acquisition, Development and Maintenance	
Expectations:	Service Providers should have and adhere to an established process for developing secure infrastructure, systems, and/or applications. Programs written should be certified as free from malicious code and patent-infringement issues and appropriate for use. The programs should also be protected from unauthorized copy, use, duplication, and storage, with asset-management requirements specified. Service Providers should ensure all proposed system changes are reviewed and tested to be sure they do not compromise the security of either the system or the operating environment.
Documents that may be requested:	• Application security policy • Network diagram • Dataflow diagram • Change control policy • Programming standard and guidelines • Certifications of encryption algorithms • Documentation of security reviews of application code • Vulnerability assessments of application and environment
Domain: Information Security Incident Management	
Expectations:	Security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. A consistent and effective approach is applied to the management of information security incidents.
Documents that may be requested:	• Incident and response policies • Log of incidents with evidence of investigation procedures and results
Domain: Business Continuity Management	
Expectations:	Service Providers are expected to have comprehensive business continuity plans, including having technology solutions that ensure recovery of services to during a time of business interruption. These plans should be tested at

	least annually and results of the tests should be made available. The Service Provider is responsible for ensuring its suppliers have business continuity programs and that those plans are included in recovery testing
Documents that may be requested:	• Business continuity plan • Technology recovery plan(s) • Testing schedule • Latest test results or generic test results • Contract • Copy of insurance declaration pages
Domain: Compliance	
Expectations:	Service Providers should establish and adhere to policies to ensure compliance with applicable legal and regulatory requirements. These regulatory requirements should reflect any international environments that must be accommodated based on processing locations. Information systems should be audited regularly for compliance with the Service Provider's security policies and standards.
Documents that may be requested:	• Third-party assessment reports • Regulatory reports • Annual reports (if a publicly traded company) • Financial statements for prior two years (audited, if available)