

# NATIONAL E-PROCUREMENT PROJECT GUIDANCE NOTES

## SECURITY

Title:	<b>Security</b>
Identification:	Describes the different types of security issues that organisations face when implementing e-Procurement and outlines realistic solutions and approaches that can be implemented to reduce the risk.
Version:	2.0
Date of Issue:	6 <sup>th</sup> February 2004
Current Status:	Final
Prepared By:	Rowena Ward, Strategic Procurement Services

## Contents

1.	Introduction and Definitions	3
2.	Technology Considerations	4
3.	Business Considerations	6
	3.1 General Issues	6
	3.2 Specific Security Considerations	7
4.	Issues and Risks	9
5.	Conclusions	10
6.	Links to Other Documents	11

## 1. Introduction and Definitions

Concern about security and privacy is one of the major factors restricting the growth of e-Procurement. In summary, an organisation should consider securing itself against:

- Damage to business reputation
- Failure to comply with internal policies, national requirements and the law
- Loss, corruption or sharing of commercially sensitive or business critical information
- Loss of business continuity due to loss of business critical systems or information
- Loss of commercial position due to inappropriate sharing of commercially sensitive information or the inability for potential suppliers to participate

In general, the types of security breaches that may occur include:

- Fraud and financial loss, including misappropriation of funds and leaking of sensitive information (e.g. pricing information)
- Lack of commercial awareness amongst employees
- Theft of data on laptops or other hardware items
- Systems being unavailable for technical or physical reasons, or because solution providers have ceased trading

This document describes the different types of security issues that organisations face and outlines realistic solutions and approaches that can be implemented to reduce the risk. It is designed to support non-technical project team members in discussions about the business issues with internal stakeholders, their IT departments and solution providers.

## 2. Technology Considerations

This section defines some of the technical terms that will be encountered when discussing security issues and how they impact on Procurement systems.

### The Internet Problem

The security problem lies in the nature of the Internet itself. The philosophy of the Internet is to enable the open sharing of data, not to be secure and restrictive. The Internet links different computers and networks together, providing public access to information and systems with little or no control. Information that passes over the Internet (i.e. anything you type into a web site, or anything that is sent electronically using the Internet infrastructure, including external emails) is transmitted through intermediate computers before it reaches its destination. This enables third parties to access it and provides an opportunity to either view or interfere with it, if it is not suitably secured.

When transferring information over the Internet you must be assured of:

- *Confidentiality* – no one apart from authorised parties can read any of the details of the transaction. To ensure confidentiality over the Internet, encryption should be used.
- *Integrity* – ensure no one has tampered with the transaction en route. This is typically done through the use of algorithms and check digits. If a transaction is found to be corrupt, then it can automatically be re-sent.
- *Authentication* – both sending and receiving parties can positively identify each other. The use of user ids, passwords and digital certificates ensures that electronic impersonation cannot occur.
- *Non-Repudiation* – evidence of the details of a transaction can be provided, so that neither party can deny it has taken place, i.e. the audit trail. Solution providers determine how this will be done in each case.

Organisations must ensure that only information that they intend to expose to the Internet is allowed to pass beyond their firewall.

### Backup and Recovery

The increasing dependence on systems and technologies for business critical processes is making organisations vulnerable. This is enhanced by the trend of using systems and technologies that are outside our IT department's immediate control. More and more systems are being hosted and managed by third parties, i.e. Application Service Provision (ASP), and delivered to end users using the Internet infrastructure. From a Procurement point of view this includes Internet services such as marketplaces, suppliers' web sites and e-Sourcing solutions, but it can also include the external hosting of core business systems such as Finance.

Organisations intending to use Internet-based solutions need to satisfy themselves that:

- System functionality is accessible at all times that it is needed by all stakeholders
- The service provider has adequate contingency plans in case of physical or technical disaster and that these are regularly tested

- You have a contingency plan which can be implemented in the case of the system provider ceasing trading (a very real risk in today's technology sector)
- Any service provider used has the same levels of confidence and contingency with its third party technology providers

Of course, the same considerations need to be made when using systems hosted internally.

### Security of Hardware

Hardware includes any devices, from servers to desktop PCs, laptops and mobile phones, which in this case form a fundamental part of the Procurement system.

The disaster and recovery strategy (see above) will protect data stored on servers; however, many organisations fail to consider the impact of losing, corrupting or inadvertently sharing business-sensitive data held on end user devices such as PCs and laptops. It is recommended that the IT security policy include references to:

- Regular backup of business-related documents such as emails, documents and spreadsheets
- Advice on protecting data on computers from unauthorised access, including the use of user ids/passwords and system locking
- Advice against using 'cookies' when accessing Internet services. Cookies are small programs that are held on a PC generally to enable a user to be recognised by a web site
- What equipment may be taken off-site and what data can be stored on those machines

Procurement policies and procedures should also stipulate where master copies of electronic documentation, such as supplier evaluation records, meeting minutes, letters, contracts and tenders, should be held.

## 3. Business Considerations

This section outlines the wider business issues that organisations need to address when designing and implementing Procurement systems. Also highlighted are examples of where security issues apply to specific Procurement system solutions.

Undertaking a risk assessment at regular stages of implementation will enable organisations to consider the most effective approach to security. Define what could go wrong, what the probability is of it happening, and what the consequences would be. Then determine what to implement (a technical or manual solution) to monitor the risk.

Determining the nature of information that is being transferred and stored will also help. Different levels of security should be considered for informal transactions, personal information and transactions carrying low or high financial or business implications.

### 3.1 General Issues

- **User Ids and Passwords**

The majority of modern Procurement-related systems will at least expect users to 'sign in' when they are to be used. Issues to be considered around user ids and passwords include:

  - Who keeps a record of current users and their passwords, and where those records are stored, electronically and/or in hardcopy form
  - The procedure for registering new users must be efficient enough to discourage the sharing of user ids
  - Strict procedures need to be applied to enable 'proxy' type activities (where one individual undertakes an activity on behalf of another), and proxy usage must be able to be monitored
  - Automated procedures around enforcing regular password changes should be applied
  - Sharing of user ids, or having 'corporate' ids for external web sites, must be prohibited
- **Updates to Master File Data (including supplier, catalogue, authorisation levels, accounting information, etc.)**
  - Ensure that only nominated system administrators have access to master file information
  - Use data range security functionality for large databases or large user bases: sub-sets of cost centres or project codes, for example
  - If possible use control reports and/or workflow for business critical data changes (if suppliers amend prices, for example)
- Explore the use of value limits, access security and workflow alternatives that solutions provide. Consider using different workflow routes to manage categories of spend differently, depending on value and risk
- Wherever possible default data from control tables to ensure maximum adherence to business rules and minimum miscoding. Examples include preferred suppliers, general ledger coding, payment terms and delivery addresses

## National e-Procurement Project – Guidance Notes

- Ensure that the appropriate separation of duties is realistically applied to deter fraud
- Ensure that an audit strategy is implemented, based on a management by exception culture. This will include spot-checking, trend and profile analysis and exception reporting. An audit strategy should be designed to ensure that there is adherence to corporate policy, but also that the organisation is receiving value for money and is performing efficiently
- Ensure that your management information strategy defines who sees what and when. For example, who has access to Purchasing Card history – the card holder, budget holder; what commercial impact is there if suppliers gain access to spend data
- Implement business awareness programmes to increase awareness of issues amongst employees. This will include data security, spotting areas of concern and basic commercial awareness

### 3.2 Specific Security Considerations

Note that this list of considerations by solution type is not meant to be exhaustive but is intended to show a summary of where security issues are most relevant.

Solution	Security Issues / Considerations
<b>Finance Systems</b> <i>Including purchase ordering, Accounts Payable, Finance and Budgeting modules.</i>	<ul style="list-style-type: none"> <li>• Segregation of data</li> <li>• Backup and recovery issues</li> <li>• Ensuring integrity of data – one version of the truth</li> <li>• Ensuring compliance with corporate and other legal guidelines (audit trails, spend analysis, etc.)</li> </ul>
<b>e-Procurement</b>	<ul style="list-style-type: none"> <li>• Internet security issues</li> <li>• System accessibility issues</li> <li>• Loss of control of critical business data</li> <li>• Effective use of workflow and limits – management by exception</li> <li>• Avoiding limiting supply base due to choice of technology</li> <li>• Ensuring adherence to contracts and corporate policy</li> <li>• Ensuring corporate policy is applied (and adapting corporate policy to include e-Procurement)</li> </ul>
<b>Buying On-Line</b>	<ul style="list-style-type: none"> <li>• Avoid the use of 'corporate' user ids</li> <li>• Ensure that delivery addresses are restricted to known business addresses</li> <li>• Prevent the use of cookies to remember user ids and passwords</li> </ul>
<b>Purchasing Cards</b>	<ul style="list-style-type: none"> <li>• Prevent the use of cookies to remember card numbers on web sites</li> <li>• Determine optimum levels of transaction and credit limits</li> <li>• Interrogate statements to provide trends and investigate exceptions only</li> <li>• Ensure Purchasing Card policy covers security of the card and personnel implications of breaches of security</li> </ul>

## National e-Procurement Project – Guidance Notes

---

Solution	Security Issues / Considerations
<p><b>e-Sourcing</b></p> <p><i>Including e-Quotations, e-Tendering, e-Auctions</i></p>	<ul style="list-style-type: none"> <li>• Establish the rules based on ethical business principles prior to starting the process, and communicate them to all parties (internal and external) – getting this wrong can impact on business reputation, and in the public sector can be against regulations</li> <li>• Where necessary, ensure bidders are evaluated prior to automating the process</li> <li>• Ensure that solutions can support business policy – sealed bids, separation of duties, etc.</li> <li>• Protect commercially sensitive information</li> </ul>
<p><b>Management Information</b></p>	<ul style="list-style-type: none"> <li>• Who has access to what and when</li> <li>• Defining ownership of data</li> <li>• Information sharing with external stakeholders</li> <li>• Compromising commercial position through inappropriate sharing of information</li> </ul>

## 4. Issues and Risks

In addition to the general issues highlighted earlier in this document, the following should also be considered:

- Good business and procurement principles can be forgotten when IT gets in the way
- Information security and negative impact on business reputation should not be seen as barriers to e-Procurement
- Avoid the “one size fits all” approach, be pragmatic about the real risks, and build checks and controls to identify and manage them. The benefits of buying on-line and using a Procurement Card far outweigh the potential issue of card misuse, for example
- Adopting a management by exception culture can be a challenge in organisations that are traditionally cautious and highly administrative
- Corporate policies and procedures are not revised to reflect the changes in culture – such as exception management and risk-based processing
- Suppliers will be reluctant to be included if security of their commercial information cannot be guaranteed

## 5. Conclusions

- Most of the issues are business issues – except for virus attacks, realistically it is unlikely that you will be impacted by hackers. Provided that basic precautions are in place (e.g. anti-virus and firewall software), there is a much greater risk of accidental or malicious damage from known sources, such as employees
- Do not let IT put you off. IT security policies can be changed, and if there is a strong business case then you will need to push the barriers. Find examples of where the organisation is already doing similar types of business transactions and use these to support your case
- Make the most of software providers' knowledge and experience, especially experiences from their customers
- Pilot and test business critical systems to ensure confidence
- Continually remind stakeholders that security begins with them
- Ensure that you consider technical, procedural and physical controls
- Do not assume that software providers have considered all the security implications, or the security of their providers. Ensure contracts and agreements include security requirements
- Remember that local authorities and their service providers are responsible for security for all users including those receiving services as a result of actions taken via any system e.g. social services clients

### 6. Links to Other Documents

The following web sites and documents provide useful additional information on this subject:

- International Standard on Information Security Management (BS7799)
- BASDA e-Business, An Overview ([www.basda.org](http://www.basda.org))
- CIPS e-Business Security ([www.CIPS.org](http://www.CIPS.org), access restricted to CIPS members only)

Prepared by:

**Strategic Procurement Services**



**Strategic Procurement Services**

**PO Box 58**

**Prudhoe**

**Northumberland**

**NE41 8ZA**

[www.strategiccps.co.uk](http://www.strategiccps.co.uk)

[info@strategiccps.co.uk](mailto:info@strategiccps.co.uk)