

Local Government Data Handling Guidelines

How Lumension Solutions Help To Reduce Risk & Ensure Consistent Best Practice Within Local Councils

By employing an application and removable device whitelist, you can ensure that only authorised personnel are able to connect removable storage devices or run authorised applications on government endpoints. Similarly, the whitelist prevents any unauthorised applications or executable files from running on government IT.

Introduction

The Local Government Association and the Society of Information Technology Management (SOCITM) published their guidelines for local council information security and data handling in November 2008. This was designed to provide a local government response to the Information Commissioner's "Data Handling Procedures in UK Government" published in June 2008.

In October 2008 the Information Commissioner, Richard Thomas reported to Parliament that a total of 277 data breaches had been reported to him in the twelve months following the HMRC loss of two CDs containing 25 million child benefit records in 2007. These information security incidents were reported from central and local government departments; the NHS; law enforcement; education; charities and the private sector. While Thomas acknowledged that this figure could reflect the fact that organisations have introduced more auditing in response to the Data Handling in UK Government Guidelines, nevertheless the local government document acknowledges that these incidents have led to a loss of public confidence in the safety of their personal information. More recently, 7,851 unencrypted children's records which were stored on a laptop stolen from the car of a Surrey County Council contractor, demonstrated that data held on portable storage devices represents a significant risk.

The Local Government Data Handling Guidelines, written by Paul Coen, Chief Executive of the Local Government Association and Steve Thomas, Chief

Executive of the Welsh Local Government Association were written for local council staff at all levels in response to high profile losses of public data.

The guidelines call for all local councils to work to recover the public's trust in the government's ability to safeguard their personal information. The guidelines reflect the good practice set out in the ISO/ IEC 2700 Information Security Management Systems and set out the fundamental steps that every council should take to mitigate risks to information.

In particular, the local government guidelines call for the appointment of a Senior Information Risk Officer (SIRO) to be appointed by each local council to ensure accountability for the protection of citizens' information. The guidelines call for councils to foster a culture where all staff recognise that personal information is a precious asset and take all reasonable steps to protect it. While acknowledging that no council can ever claim to be immune from data security breaches, the local government document defines best practices that all councils must strive to consistently meet or exceed, so that the public can be reassured that all reasonable steps have been taken to protect their information.

The following document provides a summary of the key parts of the local government guidelines and demonstrates how the Lumension solution portfolio helps local councils to ensure that best practice is consistently followed when assessing and removing risks to citizens' information.

Local Government Data Handling Guidelines:

Undertake regular risk assessments.

Councils should undertake regular risk assessments to ensure confidentiality, integrity and availability of the information they hold. There should be clear records of the assessments conducted and these should be shared and discussed with senior management.

How Lumension helps UK local councils to meet the guidelines

Lumension Vulnerability Management™ allows local councils to assess the risk to their IT systems against known vulnerabilities. When Lumension Vulnerability Management is used, the council's system can be compared to secure system configurations, providing council IT managers to plan and remedy any known vulnerabilities. Lumension then generates reports to provide both management level and low level detail, ensuring that risk assessment and risk remediation plans are available for all key stakeholders within that local council.

Lumension Endpoint Protection™ applies a whitelisting approach, whereby only known and trusted applications are allowed to run on a local council's network. Every other file or application is blocked by default. This minimises the risk of unlicensed or malicious software being introduced to the council's network and compromising data held within it.

This whitelisting approach ensures that data added to the network complies with best practice guidelines and that only council approved and trusted applications are being run on its network.

Lumension Data Protection™ also whitelists devices, ensuring that only known and approved storage devices can be connected to the council's network. This reduces risk to data by enforcing council policy, such as use of encryption on devices and ensuring that only certain council employees can use storage devices.

Detailed logs on all data moved to and from USB memory sticks; laptops and CD are created in Lumension Data Protection. This provides a clear record of any attempt to subvert the council policy on removable storage media as well as auditing how approved media and applications are being used.

Local Government Data Handling Guidelines:	How Lumension helps UK local councils to meet the guidelines
<p>Ensure the secure disposal of information.</p> <p>All personal information should be securely destroyed: paper records by incineration, pulping or shredding so that reconstruction is unlikely and electronic media by overwriting, erasure or degaussing for re-use. This is in accordance with government guidelines. Where possible, a CCTM5 approved product or service should be used.</p>	<p>The PGP Shredder feature within Lumension enables council staff to destroy data sent to the Windows Recycle Bin by various methods to ensure that data cannot be recovered.</p>
<p>Wherever possible councils should avoid the use of removable media including laptops, removable discs, CDs, USB memory sticks, PDAs and media card formats.</p> <p>Where it is unavoidable, encryption should be used and the information transferred should be the minimum necessary to achieve the business objective.</p>	<p>Lumension Data Protection provides the ability to control all device types, down to a serial numbered device to ensure tight controls over who can store information on removable storage media.</p> <p>If users do require the ability to write to removable media, Lumension Data Protection can be used to enforce encryption on USB and CD/DVD disks to ensure that it is not possible for a user to write unencrypted data to the device.</p> <p>Lumension Data Protection allows council IT administrators to set copy limits and file type filtering (content filters) to ensure only approved file types can be imported or exported to and from approved media types. The copy limit ensures that only the necessary amount of information can be copied. This prevents entire databases from being stored to removable media, where only a few records are required for the task at hand.</p>

Local Government Data Handling Guidelines:	How Lumension helps...
<p>Work towards a policy of least privilege.</p> <p>Wherever possible, access to systems should be restricted to those users that need it. Access to raw data should be strictly controlled and where possible, only anonymous data should be readily available. Use of the cross-government Employee Authentication Service is an option which should be considered.</p>	<p>Lumension Endpoint Security Suite™ (which includes both Lumension Endpoint Protection and Lumension Data Protection) provides local council staff with minimal access to applications and data, by default.</p> <p>Additional access privileges are only granted via the system administrator to specified individuals using approved devices and applications. This enables all network access to be strictly controlled, monitored and logged. If an application or device is not specifically approved by the system administrator and added to the whitelist of sanctioned applications and devices, no user will be able to use it on the council's IT system.</p> <p>Data access controls can be further reinforced using PGP NetShare. This allows the IT administrator to restrict user access to data beyond standard NTFS shares. If the user has not been given explicit access using a trusted PGP Key they will not be able to access the data, even if NTFS permissions allow them to see the encrypted file.</p>
<p>Personal information should be kept within secure premises and systems.</p> <p>Where it is not possible to access information on secure premises and systems, the following hierarchy should apply:</p> <ul style="list-style-type: none"> • Access should be via secure remote access so that information can be viewed or amended without being permanently stored on the remote computer. • Next best is secure transfer of information to a remote computer on a secure site on which it will be permanently stored. • Decisions on handling/transfer of information should be approved in writing by the relevant information asset owner. • User rights to transfer information to removable media should be carefully considered and strictly limited. 	<p>Where storage of information on a computer cannot be avoided, Lumension's integrated PGP NetShare (for network share storage) and PGP Whole Disk Encryption (portable devices) can be used to ensure data cannot be accessed by anyone other than approved personnel.</p> <p>Where the use removable media cannot be avoided, Lumension Data Protection can ensure that media is fully encrypted. Copy limits and file type filters can be used to ensure only council approved data is transferred for greater protection of citizen data and to enhance the public's trust in the council's handling of their personal information.</p>

Local Government Data Handling Guidelines:	How Lumension helps UK local councils to meet the guidelines
<p>All councils should engage independent experts who are members of a TigerScheme, Crest, or CHECK to carry out penetration testing of all ICT systems where it is deemed necessary.</p>	<p>Lumension Scan™ is an admin-access vulnerability assessment tool used extensively by organisations to prepare for and defend against penetration testing activities.</p>
<p>New ICT systems should be accredited to Government standards For new systems containing personal information, councils should aim to have systems accredited to Government standards.</p> <p>When procuring new systems, councils should also consider putting in place arrangements to log activity of users in respect of protected personal information and for asset owners to check it is being properly conducted.</p>	<p>Lumension Data Protection provides a detailed audit trail of all data that is transferred by sanctioned personnel using patented bi-directional shadowing for all council staff or particular groups of users.</p> <p>Lumension Data Protection delivers centralised management and clear visibility of device usage and data transfer to and from devices for the entire network.</p> <p>Any attempt to access or transfer data onto removable media is logged within Lumension's audit trail and a detailed report of every device that has ever been connected to the network can be produced.</p>
<p>Produce a Corporate Information Risk Policy.</p> <p>The policy should set out how to implement the measures in this document in relation to council's activities and that of delivery partners, and monitor compliance with the policy and its effectiveness.</p>	<p>Lumension's whitelist approach enforces council policies regarding the use of applications and removable storage devices. By default, all users are given minimum privileges and all access has to be specifically sanctioned by the council's IT administrator. This reduces risk to information caused by malware introduced through applications or devices as well as the loss of removable storage media.</p> <p>The reporting capabilities found in both Lumension Vulnerability Management and Lumension Endpoint Security Suite enable council managers to monitor compliance of the overall policy, including adherence to maintaining an up to date deployment of known fixes to vulnerabilities and where users have tried to circumvent corporate policies with regards to application and device usage.</p>

Local Government Data Handling Guidelines:	How Lumension helps UK local councils to meet the guidelines
<p>Complete Corporate Information Risk Plans (review and forward looking) .</p> <p>At least once a year complete a Corporate Information Risk Plan, review all assessments and examine forthcoming potential changes in services, technology and threats.</p>	<p>Reviewing the comprehensive logs and reports provided by Lumension's solutions will enable councils to identify areas where policies are being followed correctly and determine where policy needs to be reinforced or even adapted to meet changes in local council or government requirements.</p> <p>Active testing of the policies could be carried out via penetration testing using Lumension's solutions. This could include using controlled experiments where unsanctioned storage devices are provided to staff to monitor how many attempt to use them (this will be blocked and logged by Lumension Data Protection). Regularly undertaking penetration testing will allow the council to identify where education on information security risk needs to be reinforced.</p>
<p>Produce a Risk Recovery Policy.</p> <p>Councils should have a policy for recovering from information risk incidents. This includes the loss of protected personal data and ICT security incidents. The policy should cover the council's media and legal response and should have clearly defined responsibilities; all staff should be made aware of the policy.</p>	<p>In the event of a loss of an encrypted removable storage device, Lumension Data Protection's audit trail can be used to identify which member staff encrypted the device and the data that was transferred.</p> <p>Lumension's patented bi- directional shadowing allows the affected council to identify all data copied from or to the removable storage device, even if the device itself was not recovered.</p>

Summary of how Lumension answers the key requirements of the Local Government Data Handling Guidelines

The Lumension Endpoint Security Suite combines Application and Device Control enabling Local Government departments and their delivery partners to centrally manage, monitor and control precisely which removable storage devices and applications are permitted to run on government networks.

Lumension Endpoint Security Suite minimises user access rights to data, applications and removable media by operating a whitelist of known, trusted and permitted applications and devices. By default, end users have no access to removable media and where this is permitted, via centralised control of the user privileges, encryption can be enforced on the data or the device. This “default deny” approach ensures clear lines of responsibility and accountability for data being transferred and fosters a culture of data security among personnel that are granted access to citizen data. All data transferred, as well as attempts to do so, are added to the Lumension Data Protection audit logs. This allows for scrutiny of departments’ data handling procedures, aids reporting and answers the requirement for all government departments to keep records in readiness for a spot check by the Information Commissioner.

Lumension Endpoint Security Suite provides centralised, policy-based enforcement of applications used on the council’s network to secure all endpoints against data loss via malware, spyware or zero-day threats. It also prevents unwanted or unli-

censed software from running on the network without the express authorisation of the local council’s IT administrator.

Lumension Endpoint Security Suite:

- » Removes the risk of data loss through the unauthorised use of removable media
- » Enforces encryption on removable media where their use is unavoidable
- » Removes the risk of data leakage or data theft as a result of unauthorised applications
- » Prevents unknown or malicious code from running, including malware; keylogger software or other spyware; zero-day threat and other destructive viruses that target systems and data
- » Audits device and application usage and creates logs of all data transferred to or from devices and by whom
- » Maintains IT system integrity and improves system performance and network bandwidth
- » Employs a whitelist approach that protects against evolving risk factors
- » Employs a whitelist approach that enables compliance with new directives or regulations
- » Improves local council staff’s productivity without increasing risk

For More Information

See how you can effectively secure government endpoints, protect data in transit, provide visibility of all policy, permissions, data transfers and audit all authorised and attempted data transfers with the leading endpoint policy-enforcement solution on the market today. For more information, to obtain a demonstration of the Lumension Endpoint Security Suite, or to enjoy a 30 day free trial, contact us.

About Lumension

Lumension™, Inc., a global leader in operational endpoint security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets.

Lumension enables more than 5,100 customers worldwide to achieve optimal security and IT success by delivering a proven and award-winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection, and Reporting and Compliance offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year.

Headquartered in Scottsdale, Arizona, Lumension has operations worldwide, including Virginia, Florida, Luxembourg, the United Kingdom, Spain, Australia, India, Hong Kong and Singapore. Lumension: IT Secured. Success Optimized. More information can be found at www.lumension.com.



United Kingdom Office

Unit C1 Windsor Place
Faraday Road, Crawley
West Sussex, London RH10 9TF
United Kingdom
phone: +44 (0) 1908-357-897
fax: +44 (0) 1908 357 600

www.lumension.com

Vulnerability Management | Endpoint Protection | Data Protection | Reporting and Compliance