NORTH LANARKSHIRE COUNCIL

AGENDA ITEM No. 2(a)

REPORT

To:	POLICY AND RESOURCES (VACANCY MONITORING) SUB- COMMITTEE	Subject:	HOMOLOGATION OF THE APPROVAL TO FILL THE POST OF ICT SECURITY MANAGER
From:	HEAD OF E-GOVERNMENT & SERVICE DEVELOPMENT		
Date:	5 July 2012	Ref:	

1. **Purpose of the Report**

1.1 The purpose of the report is to seek homologation of the decision to approve the filling of the ICT Security Manager post (NLC13).

2. **Background**

2.1 Within EGASD the post of ICT Security Manager is vital in light of the importance of this role in terms of our Information Governance. The current ICT Security Manager is due to retire on 31 July 2012.

2.2 In view of the need to fill the post of ICT Security Manager as a matter of urgency, the Chief Executive, following consultation with the Convener, approved the filling of the post, on the basis that this decision would be homologated at the next meeting of the Sub-Committee.

3. **Recommendation**

3.1 It is recommended that the Sub-Committee homologates the action taken to fill the post of ICT Security Manager (NCL13).

Irene McKelvey

Head of E-Government & Service Development

For further information please contact Irene McKelvey, on tel. ext. 2532

Policy and Resources (Vacancy Monitoring) Sub-Committee

Request to Fill a Vacancy Graded NLC12 and Above

Service: Finance and Customer Services	**Division: EGASD**
Section: ICT	**Post: ICT Security Manager**
Grade: NLC 13	**Current Salary Scale: £ 34,683 - £ 41,823**
Date vacancy occurred: Post due to be vacated 31 July 2012	
Reason for vacancy: The current ICT Security Manager is due to retire.	

What are the consequences of not filling this post?

This is a vital role within the organisation and would put us at risk if any high profile incident occurred at a time when we did not have a dedicated professional in place.

The ICT Security Manager chairs the Information Security Forum (ISF) which has representation from All Services. This forum supports promotion of the Information Security Policy and Security awareness across all areas of North Lanarkshire Council. All breaches of information security, actual or suspected, must be investigated and this role is where that responsibility lies.

The ICT Security Manager is the designated owner of the Information Security Policy and is responsible for it's ongoing maintenance and review as well as producing the associated Standards, Guidelines and Procedures

The ICT Security Manager serves as our internal security consultant. They are responsible for ensuring that the appropriate focus is maintained to protect the Council by developing the ICT security policy in line with the changes in legislation and technology. This role provides authoritative advice and guidance in the application and operation of all types of security control including regulatory requirements.

The different types of incidents that we need to be aware of and ensure procedures are in place for include: theft or unauthorised disclosure of confidential information; attack or unauthorised access by outsiders; infection by malicious software; infringements of laws or regulations; physical theft of computer equipment; fraud or theft using computers; systems failures or data corruption.

The Council requires to be constantly vigilant in this age of information becoming ever more accessible. The more visible we become to the public, the higher the risk of a significant hacking attack. ICT security failings tend to be a result of a combination of people, processes and technology

There have been numerous instances of data breaches that have resulted in organisations reputations being damaged and fines being imposed. Recent public sector instances in the press include: £140, 000 charge imposed on Midlothian Council for repeated sensitive data loss; and an unencrypted laptop containing the names, addresses and bank details of thousands of people and businesses was stolen from Glasgow City Council, this is under investigation by Strathclyde Police and the Information Commissioner's Office. The Information Commissioner's Office holds the power to issue fines of up to £500,000 for serious breaches.

As the range of threats to the security of our information expands and the variety of devices and technologies we make available to staff increases, the greater the requirement to ensure that we are taking the most robust approach to this that we can.

What alternatives to filling the post have been considered and why is it considered that these alternatives are not appropriate? It was not considered appropriate to have other members of the ICT section cover for this area as it requires specialist skills and requires full time focus. The whole area of ICT Security and Risk is ever expanding and demands concentrated effort to maintain the levels of controls required.

The following documents are enclosed with this form: **(✓)**

1. **Job Description** ✓

2. **Organisational Chart (detailing location of post in structure and including number of posts at same level)** ✓

I confirm that, for the reasons set out above, that the filling of this vacancy is considered essential.

Signature Executive Director: _____ **Date:** 27 June

Human Resources use:

Date of Vacancy Monitoring Sub-Committee _____

APPROVE / NOT APPROVE / CONTINUE

North Lanarkshire Council
Job Description

Department: Finance
Division: E-Government & Service Development
Job Title: ICT Security Manager
Post Reference:
Responsible to: Service Delivery Manager
Grade: GR13
Conditions of Service:

Job Outline:

To manage and provide expert advice on the selection, design, justification, implementation and operation of technology and information security controls and security management techniques relating to any aspect of information systems.

Main Duties and Responsibilities:

1. Serve as an Internal Security consultant to the Council
2. Create and continually develop Council Information Security Policy, and Information Security Management System
3. Monitor changes in legislation and accreditation standards that affect Information Security and propose appropriate strategies to ensure Council's continued performance.
4. Develop ICT/IS security policy, standards and guidelines appropriate to business, technology and legal requirements and in accordance with best professional and industry practice.
5. Prepare and maintain a business strategy and plan for Information Security work which encompasses any evolving risks and control requirements and is consistent with relevant Council plans and strategies.
6. Provide authoritative advice and guidance in the application and operation of all types of security control including regulatory requirements.
7. Provide a centre of ICT/IS security expertise for the organisation.
8. Act as a focal point for reporting and management of any EGASD related security incidents from tracking, to resolution, to ensuring the implementation of any enhanced mitigation.
9. Act as the focal point for reporting of any non-EGASD related security incidents providing advice and guidance on resolution.
10. Co-ordinate production and continued review of ICT Continuity Plans and supporting documents.
11. Provide assistance to Services regarding the creation of Service specific Information Security policies or Business Continuity plans.
12. Co-ordinate production and continued review of EGASD Risk Register and supporting documents.
13. Maintain broad understanding of ICT related security threats and mitigation options.

This job outline is intended to indicate the broad range of responsibilities and requirements of the post. It is neither exhaustive nor exclusive but, while some variation can be expected in particular duties, the outline is considered to provide a reasonable general description of the post.

E-GOVERNMENT AND SERVICE DEVELOPMENT DIVISION
PROPOSED ICT STRUCTURE FOR CONSIDERATION AT COMMITTEE 15 DEC 2011