Nottinghamshire County Council

Security Administration and access Control

TO ALL IT USERS

"Nottinghamshire County Council (NCC) continues to place increasing reliance on its computer systems and networks.

Everyone within NCC has a responsibility to control risk and to report errors in judgement or procedure where they see them. Doing so reduces our exposures and helps to maintain our client image.

This policy document has been agreed by ICT Executive Group and approved by the County Council. It outlines your responsibilities in respect of the computer systems you use. Adherence to it is each person's individual responsibility."

Wilful or negligent disregard for these policies will be investigated and may be treated as a disciplinary matter.

Mick Burrows
Chief Executive

1 Security Administration and Access Control

1.1 Intent

Nottinghamshire County Council (hereafter referred to as NCC) will manage, administer and control access to its computer systems in a secure manner. This will ensure that access to systems is provided rapidly to those with a genuine business need and valid authorisations, and prohibited to those without. Procedural controls will be placed around the security administration process itself to ensure that security is not undermined by misuse of privileged functions.

The strength of controls will be commensurate with the agreed risk to the business and reflect a cost effective balance between risk reduction and operational efficiency. The controls will be adjusted as necessary when risks change.

1.2 Scope

This policy applies to both networked and stand-alone systems, and extends to laptops, voice mail and other services requiring administration and access control.

1.3 Key Issues

- Implementation of a standard baseline of access control for **all systems** to allow NCC to demonstrate its commitment to proper standards of security management.
- Effective prevention of unauthorised access to systems/data, whilst being as unobtrusive as possible in normal use.
- Monitoring of events that might indicate an actual or attempted abuse of access rights.

1.4 Objectives

- To satisfy all relevant regulatory requirements imposed on NCC.
- To enable timely access to information by authorised persons.
- To provide individual accountability for system activity.
- To reduce (to an acceptable level) the risk of serious financial loss, loss of client confidence or other serious operational or business impact as a result of a failure in security.
- To demonstrate that a responsible approach has been taken to protecting the interests of clients, suppliers, joint ventures and other stakeholders in NCC.

1.5 Principles

The management and administration of computer systems will incorporate the following principles. Additional principles apply where remote access will be provided to NCC's systems. These are described in the *Remote Access Security Policy*.

- Responsibilities for security management and administration will be clearly assigned, and training provided where appropriate.

- All systems will have a nominated System Owner (and delegated alternative) to specifically authorise access.
- Written Security Operating Procedures (SOP's) will be produced as and when required. These will define the basic rules of user access, including those necessary to avoid a breach of compliance.
- All users will be authorised by the System Owner (or alternate) using standard procedures. IT Service Desk staff will not process any access requests that are not accompanied by the appropriate authorisations or which breach the written access rules.
- An audit trail will be kept of all authorised instructions.
- A minimum standard of technical access control, authentication and security auditing mechanisms will be used for all systems, including networked, stand-alone and laptop systems.
- All users will have individual user-id's, which will require authentication before access is granted to systems (usually by secret password), unless special exemption is agreed in writing by the IT Security Manager. .
- Privileged access levels will require specific authorisation from senior management. Privileges assigned will be the minimum required.
- All user access rights will be reviewed and confirmed with the System Owner at least annually.
- The use of emergency access routines to access business data will be minimised and will require the prior authorisation of designated System Authorisers (or someone delegated by the system authoriser). Audit trails covering the emergency access activity must be created and retained.
- Use of highly privileged access to production systems will be restricted to, or supervised by, authorised IT system management staff for essential support and maintenance functions. Audit trails covering the use of highly privileged access must be created and maintained.
- Requests for password re-sets (where the original password has been forgotten) will only be actioned for authenticated user requests.
- A centrally organised mechanism will be established for notifying the IT Service Desk of new starters, leavers and transfers before they occur. Housekeeping will be undertaken on a regular basis to remove dormant users and to ensure that leavers and transfers are properly recorded. Suspension of privileged functions and remote access rights from leavers will be a high priority.
- A procedure will be in place to handle reporting and escalation of security incidents.

1.6 Responsibilities

- **System Managers** will ensure that systems are implemented, operated and maintained in accordance with this policy and associated standards.
- **System Owners** are ultimately responsible for providing clear authorisation for all business users and for periodically re-verifying the propriety of the access rights assigned. This authority may be

delegated to System Authorisers at a practicable level of line management.

- **System Authorisers** will provide clear instructions to **Security and Access Team** on the set up of users and the assignment of associated access rights.
- **Security and Access Team** will ensure that user profiles and logical access controls are implemented in accordance with authorisations from System Owners and with this policy.
- The **Security Manager** will provide technical and procedural guidance on the adequacy of existing procedures, and on the options for improving security controls where necessary.
- **All staff** are responsible for maintaining the secrecy of their passwords and for notifying management of security incidents and breaches.