



Great Yarmouth Borough Council System Access & Password Policy

Author	Geoff Jones
Date	17 March 2009
Version	2.1
Last Review Date	2 March 2011
Review Changes	None
Document Status	Final

1.0 INTRODUCTION	3
1.1 POLICY RATIONALE	3
1.2 SCOPE	3
1.3 PRINCIPLES	3
2.0 SYSTEM ACCESS & PASSWORD POLICY	4
2.1 COMPLIANCE REQUIREMENTS	4
2.2 POLICY ENFORCEMENT	8
COMPUTER SYSTEMS REGISTRATION FORM	9
3.0 IMPLEMENTATION AND COMPLIANCE	10
3.1 IMPLEMENTATION	10
3.2 COMPLIANCE	10
4.0 EQUALITY IMPACT ASSESSMENT	10
5.0 HEALTH AND SAFETY	10
6.0 REFERENCE DOCUMENTS	11
7.0 DISTRIBUTION	11
8.0 REVIEW	11

1.0 INTRODUCTION

This policy forms part of the suite of policies dealing with data security.

The use of IT networks and systems within Great Yarmouth Borough Council is an essential business requirement to keep in step with the demands for the retrieving, collating and communicating of information, in a fast, economic and secure manner.

The aim of this System Access & Password policy is reduce the risk to the integrity of the resources and reputation of Great Yarmouth Borough Council, while maximising the use of these important business tools.

1.1 POLICY RATIONALE

At the time of the writing of this System Access & Password policy in 2009, the council was aiming to meet the requirements to obtain and use a government connect secure circuit.

In 2009, the Council was of the view that there was a need to ensure that an agreed standardised approach was being taken to System Access & Passwords, in order to protect Council assets, and to ensure compliance with audit requirements.

This policy seeks to establish a standard set of conditions, and a framework for System Access & Passwords within the Council.

1.2 SCOPE

This Policy will apply to all Council employees.

1.3 PRINCIPLES

The Policy is designed to ensure that there are clear internal arrangements for the effective management of System Access & Passwords.

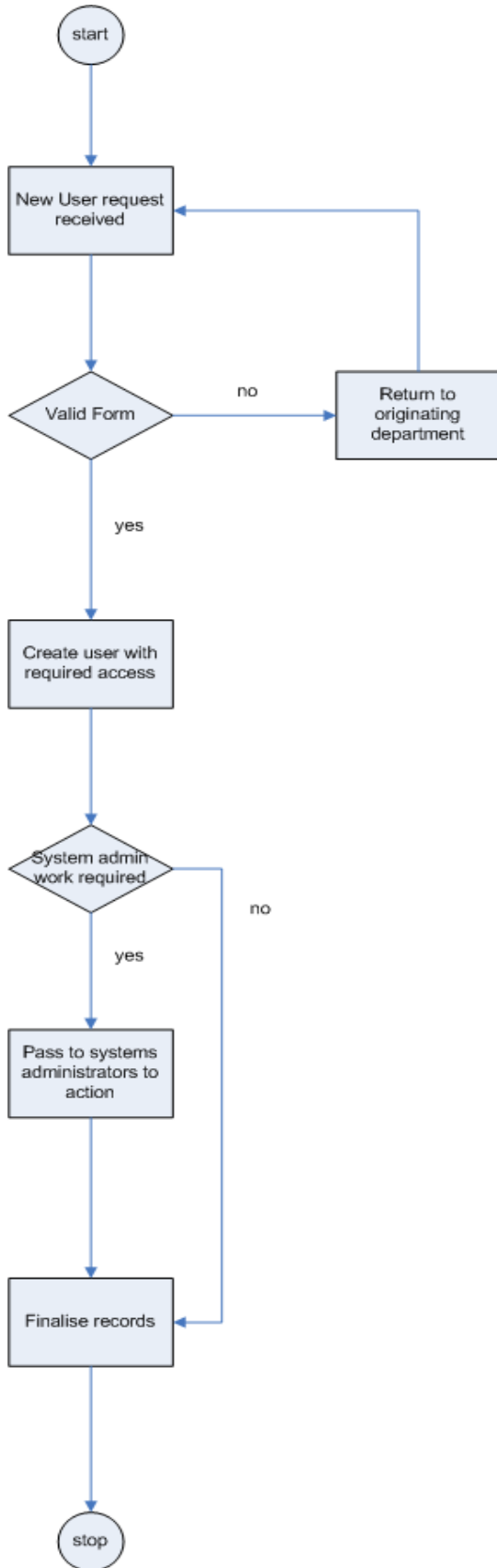
2.0 SYSTEM ACCESS & PASSWORD POLICY

2.1 COMPLIANCE REQUIREMENTS

All users must be registered to access the council's network. Staff will only be registered to access the council's network upon receipt of a computer registration form signed by the staff member and countersigned by their manager.

The computer registration form will detail the systems to which access is requested. The administrators of each system will create the appropriate access and sign to confirm this has been done, the administrators will also determine that the requested access is appropriate for the section or department.

The ID of each user must be unique and will consist where possible of three initials from the user's given names. Should this not be possible, the user only has two given names for example or the combination is already in use then a suitable agreed alternative will be issued.



Passwords are the personal responsibility of each user. You must only use your own password to access the network. Passwords should not be written down nor shared with any other party.

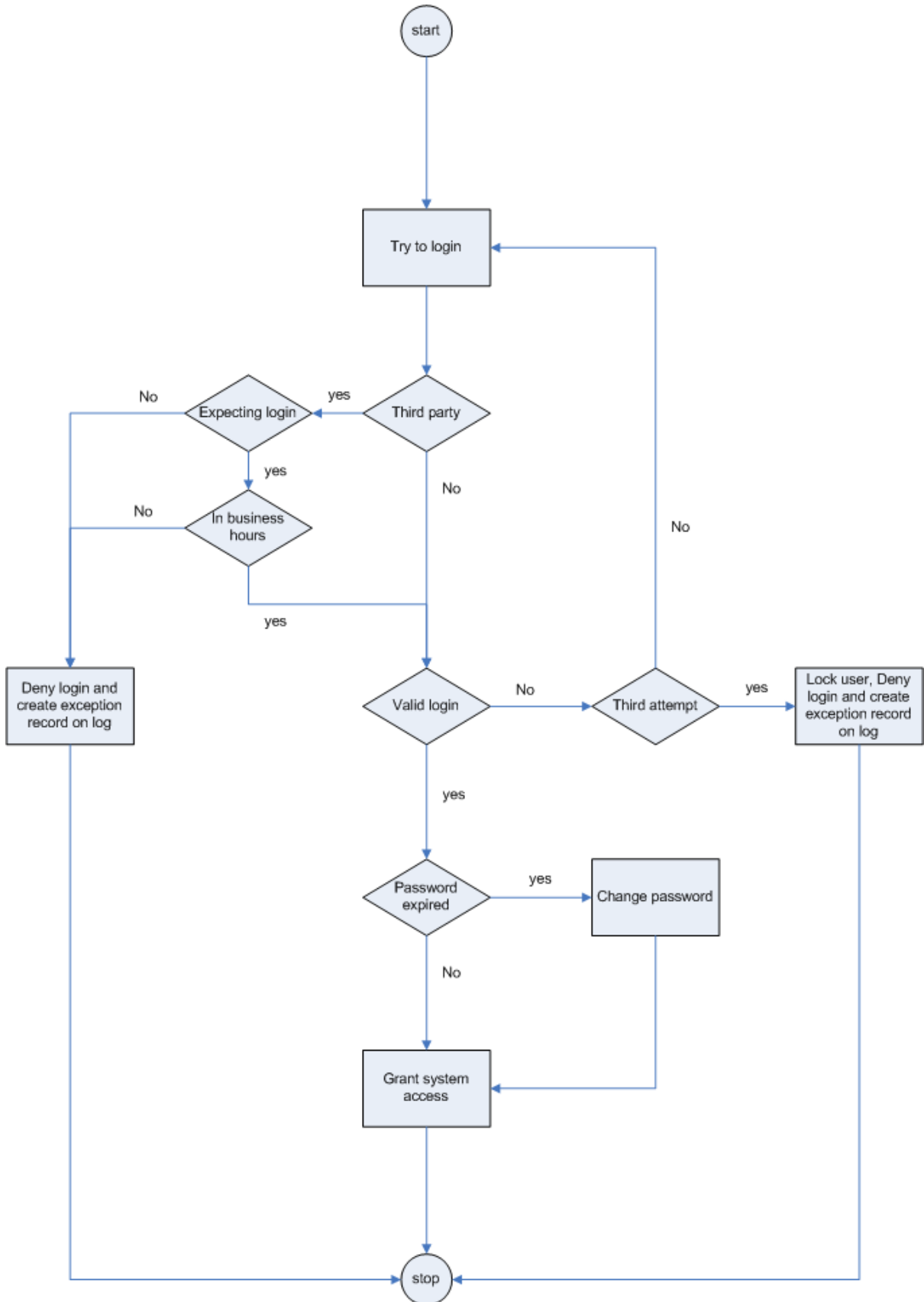
Passwords must at all times be kept private and secure and changed every 30 days. Passwords must be complex consisting of eight characters at least one of which must be a numeric and a combination of upper and lower case must be used. Passwords must not be reused. All network and system activity can be logged; this is referenced and stored with the user ID for this reason passwords and user ID's cannot be shared.

If you have reason to believe that the security of your password has been compromised you should inform the ITSS service desk immediately and change your password.

When you leave a PC you are using you must lock the system or logoff even if you are only leaving the vicinity for a short time, remember if someone uses your ID and password any activity will be logged against your name.

Companies that support systems will only have access to the servers hosting the applications they supply. They will if required be granted local admin rights to the server(s) hosting the applications but they will not have domain admin rights.

Access to the council's network for third party support will be restricted to when fault calls are raised or access is requested by the supplier. Unless requested by the supplier links will be terminated outside of business or agreed support hours as documented in their SLA. All fault calls and requests for access must be via the support desk.



2.2 POLICY ENFORCEMENT

To ensure compliance with this policy network system policy will enforce some elements automatically, however this does not negate the user's personal responsibility for adherence with the overall aims.

The following will be automatically enforced by the system:

- Password change - every 30 days
- Password being complex – minimum 7 alpha-numeric characters and 3 for the 4 following apply, at least 1 must be uppercase, 1 must be lowercase, 1 must be numeric and 1 must be a special character.
- Password expiry – 1 week reminder
- Password history – last 20 passwords
- Screens will lock after ten minutes of inactivity.

If a user fails to renew their password or enters an incorrect password three times in succession their account will be locked. The user will need to contact the support desk to get this released. This will only apply to the active directory, systems that have local passwords and do not authenticate to active directory must use password controls as close to this standard as the system allows. Access to the system will still be via the council's network and the above restrictions will still apply.

Computer Systems Registration Form

PLEASE COMPLETE IN BLOCK CAPITALS

Initials			
Full Name			
Job Title			
Dept/Section			
Telephone No:			
Payroll Number:			
Contract {Please Tick}	Permanent	Temporary	Contractor

Systems Required	Please Tick where Appropriate
OHMS/Anite	
IBS Revenues	
Ocella	
CHRIS21	
Procentre	
Integra	
Comino/Civica	
Domain Network	

I hereby confirm to have read and understood the IT Security Policies of the Great Yarmouth Borough Council and hereby formally confirm to abide by it at all times. I understand that any deviation from the policies will be reported to Management

User Signature		Date:
<i>I authorise the above mentioned employee to have access to the systems required</i>		
Managers Signature		Date:
<i>{Manager Please Print Name}</i>		

Please give User ID of existing User that has the access rights that you require			
--	--	--	--

Check list - ITSS	Check List – Dept Admin	Check List – Dept Admin
Date:	Date:	Date
Signed	Signed	Signed
ID Given	ID Given	ID Given
Access Given	Read	Read
	Update	Update
	Admin	Admin

ITSS – Use Only	Sunrise		PACE
-----------------	---------	--	------

3.0 IMPLEMENTATION AND COMPLIANCE

3.1 IMPLEMENTATION

This policy will initially be implemented through the Chief Executive and Corporate Directors of the Council.

A memo will be sent to all HOD's and SUM's to make them aware of the policy.

It is the responsibility of managers to ensure that new staff receive information about this Policy, and should be part of any local induction where appropriate. Human Resources will add the Policy to its list of policy issues provided to any new starters. Managers must also ensure that any changes to this policy are effectively communicated within their areas of responsibility.

3.2 COMPLIANCE

Managers are responsible for ensuring that staff are aware of the location of this policy. In addition, Managers are responsible for keeping staff up to date about any changes within the policy.

All staff are obliged to adhere to this Policy.

4.0 EQUALITY IMPACT ASSESSMENT

An equality impact assessment has been undertaken for the suite of policies relating to data security.

The result of this assessment shows low relevance in relation to specific equality issues and factors.

The full assessment can be found at:

<I:\Equality & Diversity\EIA\Equality Impact Assessments\Gov Connect\data security EIA.doc>

5.0 HEALTH AND SAFETY

There are no health and safety implications with this policy.

6.0 REFERENCE DOCUMENTS

This Policy should be read in conjunction with the following legislation, regulations and Council policies:

- COCO security checks
- Data Handling and Security Breaches
- Internet Security
- Email Usage
- IT Security
- Using Removable Media
- Contractors / Suppliers connecting to the GYBC network
- Taking GYBC computer equipment abroad

7.0 DISTRIBUTION

This Policy will be available for all the Council's designated locations. Copies will also be available from the 'I' drive and on the Council's Intranet.

8.0 REVIEW

This Policy will be reviewed on an annual basis with the next review date being April 2012.