UNIVERSITY OF PORTSMOUTH

GENERIC USER ACCOUNTS

April 2016

Contents

Document title		
Normal text		
Document author and department		
Normal text		
Approving body		
Normal text		
Date of approval		
Normal text		
Review date		
Normal text		
Edition no.		
Normal text		
ID Code		
Normal text		
Date of effect		
Normal text		
EITHER For public access online (internet)? Tick as appropriate		**YES**
For public access on request copy to be mailed Tick as appropriate	**NO**	**YES**
OR For staff access only (intranet)? Tick as appropriate		**YES**
Password protected Tick as appropriate	**NO**	**YES**
External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk		

If you need this document in an alternative format, please email corporate.communications@port.ac.uk

The latest version of this document is always to be found at:

https://erecords.port.ac.uk/documents/qA43279

Summary

What is this document about?

A generic account is a computer account that is not uniquely owned by an individual user. It might be used by a number of individuals who share the same password. Ideally, user accounts should be uniquely owned so that account activities can be attributed to a specific person (with a reasonable level of assurance). However, there may be circumstances where generic accounts are necessary - subject to controls. This advisory sets out the main risks arising from the use of generic accounts and the risk mitigating controls necessary if their use is authorised.

Who is this for?

This advisory should be followed by all individuals who use generic accounts on University of Portsmouth IT network or telecoms systems.

IT systems which fall within the scope of compliance of the Payment Card Industry Data Security Standard (PCI-DSS) must not have generic accounts enabled.

How does the University check this is followed?

Annual review of this advisory will evaluate the relevance of its content and the appropriateness of its scope and applicability.

Who can you contact if you have any queries about this document?

Any questions about should be directed to servicedesk@port.ac.uk

1.0 Generic Accounts - The Risks

Generic accounts are a security risk. This risk can be reduced if generic account holders follow some basic safe working practices (see 3.0). However, the risk cannot be eliminated entirely and any residual risk remains the responsibility of the ‘risk owner ’(the line manager responsible for the generic account holder).

There are some well-known security risks arising from the use of generic accounts:

1.1 Accountability - individual actions and account activity is not traceable so there is no way to prove that an individual performed a specific action.

1.2 File privacy - there is no way to achieve cross-user account security and protect the privacy of users that might have access to the generic account.

1.3 Information currency - All users have access to the same information storage and they can read, write, duplicate, delete or corrupt that information.

1.4 Password security - Generic account passwords tend to become widely known outside the group of authorised users. The passwords to a generic account should be changed each time an account user no longer needs access or is de-authorised from using that account.

2.0 Why would anyone need a generic account?

Some commonly cited reasons are listed below:

- Account access may be required by a group of people (e.g. reception desk)
- Staff turnover might be very high in a particular role.
- Events such as registration and conferences take place – ta and cf accounts
- Generic accounts may be restricted to simple tasks (e.g. data logging)
- Generic accounts may be restricted to special purposes in research areas
- The computer interface is entirely menu-driven and/or embedded.
- Activities are inherently anonymous (e.g. kiosks and data entry screens)
- Technical constraints (aka poor design) might require a generic account.
- Inflexible working processes may necessitate a generic account.

3.0 Safe working practices

3.1 Generic accounts must be assigned to a **risk owner** - This is the individual nominated as being operationally responsible for the account(s) on a day to day basis. The risk owner must create and enforce a **Local Safe Working Practice** document (see template at Appendix 1) which sets out the recommended local arrangements for the safe use of generic accounts. Please contact Information Services for help in constructing this document (ext 7777).

3.2 Generic accounts should be provided only in exceptional circumstances and will not be made generally available. They should only be issued after all other options have been given serious consideration and ruled out.

3.3 Generic accounts will be deleted by IS when the account expires, or at the request of the risk owner.

3.4 Risk owners are responsible for the assessment of business risks arising from the use of generic accounts and are responsible for the security breach if the accounts are abused.

3.6 Generic accounts must only be used on a specified workstation or workstations in a confined area such as a reception desk or small office.

3.7 There should be an agreed way of communicating the password privately to eligible staff and this password should be changed every 90 days. Password change should take place if the password is shared outside the authorised users or if an authorised user leaves post.

3.8 All generic accounts must be protected with a strong password and that password must not be shared outside the designated account users.

3.9 Individual generic accounts (single user only) must be signed over to a named individual in an auditable fashion, so that it is always possible to identify who was using an account at a particular time.

3.10 Generic accounts must not be issued to 3rd parties and non-members of the University.

3.11 Generic accounts will be reviewed every year to establish if there are grounds for continued use.

Appendix 1 Template for Local Safe Working Practice

***Title: e.g. Department/Faculty* Casual Staff ' *–Hot-Desk'* Account Access Policy**

Background

Blurb……….

Casual staff need access the UoP network through a user account on the staff domain - individual accounts are not fit for purpose in this regard. The proposed solution involves creating generic 'Hot-Desk accounts and issuing these accounts to individuals/students. Generic accounts create an increased risk because the University may not be able to trace activity to an individual account holder if asked to do so. The following safe working practices must be followed by ………….

………….end of blurb.

Safe Working Practices

The following arrangements must be in place to assure security:

1. ...the dept... will issue and revoke Hot-Desk accounts to casual staff as required.
2. ...the dept... will keep a record which clearly links a person by name to a unique Hot-Desk account.
3. ...the dept... will be accountable for the activities traceable to Hot-Desk accounts.
4. ..n.. Hot-Desk accounts will be issued to 'regular 'casual staff
5. ..n.. Hot-Desk accounts will kept aside for issue by ...the dept...at short notice.
6. Casual staff will be held responsible for all activities traceable to their assigned account.
7. NEVER share your Hot-Desk account password with anyone – UNDER ANY CIRCUMSTANCES.
8. Hot-Desk accounts are for ...department... work purposes only.
9. Only GoogleMail and GoogleCalendar are to be used on Hot-Desk accounts.
10. Casual staff must log on to their account at the start of their shift and log off at the end of their shift. Working hours must be recorded with ...the dept... separately.
11. Hot-Desk accounts will only be issued to …….. on a regular engagement with ...the dept....
12. Account holders must inform ...the dept... if they no longer wish to continue in their role.
13. During the vacation period, all Hot-Desk accounts will be locked.

University of Portsmouth
Department of Human Resources
University House
Winston Churchill Avenue
Portsmouth PO1 2UP
United Kingdom

T:	+44 (0)23 9284 3141
F:	+44 (0)23 9284 3122
E:	university.secretary@port.ac.uk
W:	www.port.ac.uk