



PROPOSED TECHNICAL GUIDE TO NRIC ADVISORY GUIDELINES

TABLE OF CONTENTS

PURPOSE OF THIS GUIDE	3
INTRODUCTION.....	4
Key Considerations for NRIC Number Replacement.....	4
ALTERNATIVES TO NRIC NUMBER	5
Option 1: User Selected Identifier	5
Option 2: Organisation Selected Identifier	6
Email Address.....	7
Mobile Number	8
Combination of Identifiers	9
REPLACING NRIC NUMBER IN EXISTING SYSTEMS	10
Preparation	10
Implementation	11
Post Implementation	12
ADDITIONAL RESOURCES.....	14
Advisory Guidelines.....	14
Other Guides	14

PURPOSE OF THIS GUIDE

This Guide aims to provide organisations with some tips for the replacement of the NRIC number as the way of identifying individuals, in their websites and other public facing computer systems.

While the topics listed in this Guide aim to provide suggestions for organisations to replace the NRIC number for identifying individuals in their websites and other public facing computer systems, the topics are not exhaustive and do not address every obligation in the Personal Data Protection Act (“PDPA”).

PDPC does not prescribe the types of identifiers that organisations should adopt in place of NRIC numbers. Organisations should assess the suitability of alternatives based on their own business and operational needs.

INTRODUCTION

The NRIC number of an individual is considered personal data as it can be used to identify the individual, and can be used to access large amounts of information relating to the individual, such as the individuals' name, address, contact numbers, income information and health information. Organisations should thus avoid the use of NRIC numbers as user names or unique identifiers in their applications, websites or public facing systems.

Examples of applications, websites and public facing systems that should use alternatives in place of NRIC numbers to identify individuals include:

- Club membership
- Loyalty programmes
- Event Management
- Online shopping
- In-store Retail membership
- Shopping Mall Car Park Redemption Kiosks

Key Considerations for Choosing a Replacement Identifier for NRIC Numbers

The replacement identifier should:

- ✓ **Be easily remembered by the individual**
- ✓ **Be unique to each individual**
- ✓ **Does not contain sensitive information**
- ✓ **Cannot be easily guessed by others**

ALTERNATIVES TO NRIC NUMBERS

This section describes some alternatives that can be used instead of the NRIC number. This includes suggestions to consider when implementing identifiers in **new** systems, and replacing the NRIC number with new identifiers in **existing** systems.

Option 1: User Selected Identifier/User Name

- Allow users to enter their own identifiers (e.g. user defined nickname).
- Ideal for systems that use NRIC Numbers as user names.

For New Systems	For Existing Systems
<ul style="list-style-type: none"> ✓ Allow each user to enter their user name during registration/account creation, or after their identity has been verified. ✓ Check that the user name is not used by another user. ✓ Check that the user name meets the organisation's system requirements, e.g. the number of characters, use of special characters. ✓ Include function(s) to help users remember or find their user name, in case they forget them e.g. option for user to request user name to be sent designated user email account or telephone number. 	<ul style="list-style-type: none"> ✓ Verify the user's identity (e.g. by getting them to log in to the system). ✓ Request the user to enter their new user name, after their identity has been verified. ✓ Check that the new user name is not currently in use ✓ Check that the user name meets the organisation's system requirements, e.g. the number of characters, use of special characters. ✓ Include function(s) to help users remember or find their user name, in case they forget them, e.g. option for user to request user name to be sent designated user email account or telephone number.

For New Systems	For Existing Systems
<ul style="list-style-type: none"> ✓ Allow each user to enter their user name during registration/account creation. 	<ul style="list-style-type: none"> ✓ Verify the user's identity (e.g. by getting them to log in to the system). ✓ Request the user to enter their new user name, after their identity has been verified.

Option 2: Organisation Selected Identifier

- Organisation selects the identifier for each user.
- Ideal for organisations that use the NRIC number internally.

For New Systems	For Existing Systems
<ul style="list-style-type: none"> ✓ Automatically generate the identifier during or after registration/account creation. ✓ Check that the identifier is not used by another user in the system. ✓ If the identifier is also a user name, to inform users of their user name after registration/account creation. ✓ Include function(s) to help users remember or find their user name, in case they forget theme.g. option for user to request user name to be sent designated user email account or telephone number. 	<ul style="list-style-type: none"> ✓ Generate a new identifier for each user, automatically. Check that the new user name is not assigned to another user. ✓ If the identifier is also a user name, to inform the user of their new user name, after their identity has been verified (e.g. after they log in). ✓ Consider a parallel run for both old and new user names to be able to be used. The duration of the parallel run may be determined based on the number of affected individuals and the frequency of access.

Email Address

- Organisation uses the email address supplied by the user as an identifier and user name.
- Easily remembered by the user.

New Systems	Existing Systems
<ul style="list-style-type: none">✓ Confirm email address during registration/account creation by getting user to enter the same email address twice, without the ability the use cut-and-paste function.✓ Check that the email address is not already used by another user in the system.✓ Validate email address by sending a confirmation link to the address.	<ul style="list-style-type: none">✓ Inform users that their email addresses will replace their NRIC numbers as their user names.✓ Have process for user to provide their email addresses if not available in existing database. Check that the email address provided is not already used by another user in the system.✓ Validate email address supplied by user, by sending a confirmation link to the address.✓ Only start accepting the user's email address as their user name, after their email address has been validated.

Mobile Number

- Organisation uses the mobile number supplied by the user as identifier.
- Like the email address, is easily remembered by the user.

New Systems	Existing Systems
<ul style="list-style-type: none">✓ Validate mobile number during registration/account creation by sending a One-Time Password (OTP) to it, and requesting the user to enter the OTP into the system. OTPs are usually randomly generated, with 6 or more digit numbers.✓ Check that the mobile number is not already used by another user in the system.	<ul style="list-style-type: none">✓ Inform each user that their mobile number will replace their NRIC as their user name.✓ Have process for user to provide their mobile number if not available in existing database. Check that the mobile number is not already used by another user in the system.✓ Validate mobile number supplied by user, by sending an OTP and checking the OTP entered by the user.✓ Only start accepting the user's mobile number as their user name, after their mobile number has been validated.

Combination of Identifiers

- Organisation uses a combination of information provided by the user as identifier.
- E.g. first name + last name, initials + last name, part name + part phone number.
- Combination should not contain sensitive personal information.

New Systems	Existing Systems
<ul style="list-style-type: none">✓ During account creation/registration, check that the combination is not already used.✓ Check that the combination meets the organisation's system requirements such as number of characters, use of special characters, etc.	<ul style="list-style-type: none">✓ Check that the combination does not belong to any other user.✓ Check that the combination meets the organisation's system requirements such as number of characters, use of special characters, etc.✓ Inform the user that the combination will replace NRIC as their user name.

REPLACING NRIC NUMBER IN EXISTING SYSTEMS

The process of replacement of NRIC numbers as identifiers and user names in websites and other public facing systems can be divided into 3 separate phases:

1. Preparation
2. Implementation
3. Post-Implementation

This section describes some suggested steps during each phase, for organisations to consider. **The steps are not exhaustive and may not apply to all organisations.**

Preparation

- ✓ Choose the NRIC replacement, and ensure that they meet the key considerations mentioned in the Introduction.
- ✓ Plan the implementation timeline, e.g. design changes to the system, system testing, notifying users, changeover period.
- ✓ Plan the steps that users will take when they replace their NRIC with the new user name, e.g. login to the system first, then enter their new username.
- ✓ Look for screens or online forms where the NRIC number is displayed, and consider whether it is required. For cases where the display is absolutely necessary, organisations should consider displaying masked NRIC numbers instead.
- ✓ Plan and design the changes to the system, e.g. new database fields for the identifier, new forms for user to enter their username, updated forms with the NRIC number removed.
- ✓ Plan and design the changes required for other systems and processes that rely on the NRIC number as a unique identifier.

Preparation (continued)

- ✓ Perform thorough system and user testing, to check that all functions for replacing the NRIC number work as designed and are user-friendly.
- ✓ Make a backup of the user database.
- ✓ Notify and educate affected parties within the organisation, e.g. customer service, so that they can plan changes to their workflow and are able to help customers during the transition.
- ✓ Plan when and how to notify users e.g. by announcement after they login.
- ✓ Ensure that the system has sufficient capacity to handle any increase in usage.

Implementation

- ✓ Ensure that all user queries are answered promptly and clearly.
- ✓ Have process in place to assist those users who have difficulties, including procedures to verify the identity of users.
- ✓ Address feedback provided by users.
- ✓ Check that users' alternate identifiers are recorded and assigned correctly.
- ✓ Monitor the number of users who have replaced their NRIC number and remind those who have not.
- ✓ Plan the processes for handling users who could not be contacted, or who could not provide their alternate identifiers during the implementation period.
- ✓ Ensure that related systems that depend on the NRIC number have also been enhanced to handle the alternate identifier.

Post Implementation

- ✓ Remind users that their NRIC numbers are no longer used.
- ✓ Conduct a review to determine whether the NRIC numbers are still required in the system as well as in the organisation.
- ✓ If not required, to remove the NRIC numbers from the system.
- ✓ Disable user accounts that do not have replacement identifiers.
- ✓ Put up a notice on the website/system, to notify users who did not change their identifiers, that their accounts have been disabled, and the process to reactivate their accounts (e.g. to contact the system administrator).

REPLACING THE PRIMARY KEY

The primary key is a unique identifier for each record in a database, and is used by the database to link records together. For example, the individual's contact details and account details may be kept in separate records. Although most systems use a database generated unique value as the primary key, some organisations have been using the NRIC number as a primary key instead.

Some suggestions and considerations for organisations who are replacing the NRIC number as the primary key in their databases include :

- ✓ Use a database generated primary key value. The database will automatically ensure that all primary key values are unique.
- ✓ If the organisation wishes to use values other than the database generated value, then the new primary key should ideally be a value that will not change over time.
- ✓ Prior to changing the primary key, organisations should identify all records that use the primary key and plan carefully for these records to be updated with the new primary key. An update to the primary key can lead to the update of potentially a lot of database tables.
- ✓ Organisations should also make the necessary enhancements to the systems and applications that use the database, e.g. CRM system, to ensure that the new primary key does not affect the functionalities of these systems and applications.
- ✓ When changing the primary key, organisations should utilise built-in database functions wherever possible.

ADDITIONAL RESOURCES

Organisations and their vendors are encouraged to refer to the following resources on the PDPC website, which provide more information on the areas that are mentioned briefly in this Guide.

Advisory Guidelines

- Can be found on the PDPC website at <https://www.pdpc.gov.sg/ag>
- Chapter 17 (The Protection Obligation) of the Advisory Guidelines on Key Concepts in the PDPA
- Chapter 18 (The Retention Limitation Obligation) of the Advisory Guidelines on Key Concepts in the PDPA
- Chapter 19 (The Transfer Obligation) of the Advisory Guidelines on Key Concepts in the PDPA
- Chapter 7 (Online Activities) of the Advisory Guidelines on the Personal Data Protection Act for Selected Topics

Other Guides

- Can be found on the PDPC website at <https://www.pdpc.gov.sg/og>
- Guide to Securing Personal Data in Electronic Medium
- Online resources on changing database primary key
 - a. IBM DB2 https://www.ibm.com/support/knowledgecenter/en/SSEPGG_9.5.0/com.ibm.db2.luw.admin.gui.doc/doc/t0023772.html
 - b. Microsoft Access <https://support.office.com/en-us/article/Add-or-change-a-table-s-primary-key-in-Access-07b4a84b-0063-4d56-8b00-65f2975e4379>
 - c. Microsoft SQL <https://docs.microsoft.com/en-us/sql/relational-databases/tables/primary-and-foreign-key-constraints>

- d. MySQL https://www.techonthenet.com/mysql/primary_keys.php
- e. Oracle
<https://docs.oracle.com/javadb/10.8.3.0/ref/rrefsqlj81859.html>
- f. Sybase
<http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.help.sqlanywhere.12.0.1/dbusage/managingprimarykeys-sql.html>
- g. TechOnTheNet
https://www.techonthenet.com/oracle/primary_keys.php
- h. W3Schools https://www.w3schools.com/sql/sql_primarykey.asp

END OF DOCUMENT

BROUGHT TO YOU BY



Copyright 2017 – Personal Data Protection Commission Singapore (PDPC)

The contents herein are not intended to be an authoritative statement of the law or a substitute for legal or other professional advice. The PDPC and its members, officers, employees and delegates shall not be responsible for any inaccuracy, error or omission in this publication or liable for any damage or loss of any kind as a result of any use of or reliance on this publication.

The contents of this publication are protected by copyright, trademark or other forms of proprietary rights may not be reproduced, republished or transmitted in any form or by any means, in whole or in part, without written permission.