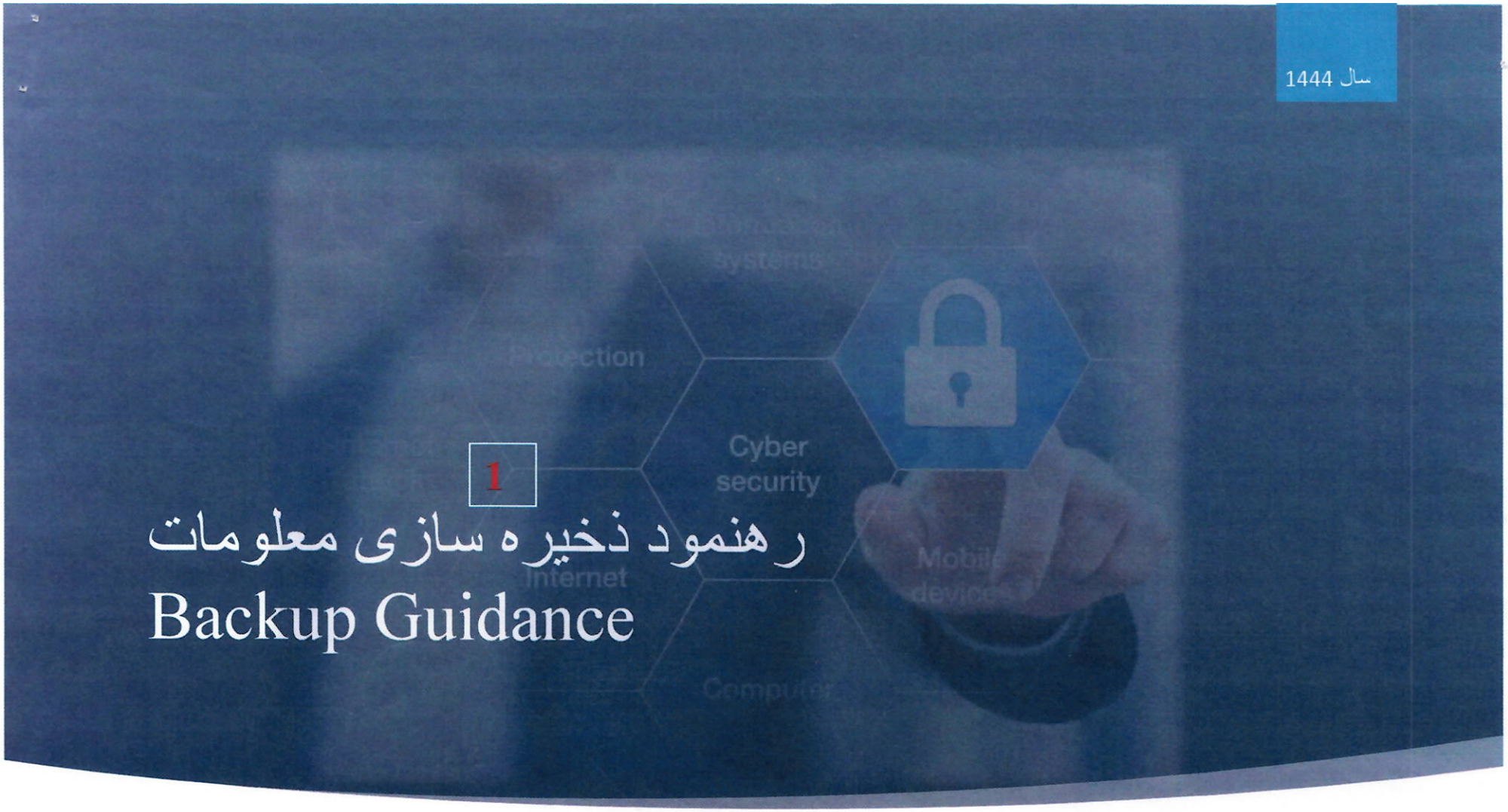
سال 1444




1

# رهنمود ذخیره سازی معلومات

# Backup Guidance

Demo

PREPARED BY ICT DIRECTORATE

MINISTRY OF URBAN DEVELOPMENT AND LAND- ADMIN AND FINANCE DEPUTY- ICT DIRECTORATE

## 1.0 Definitions:

- **Backup** – To copy data to a second media, solely for the purpose of safe keeping of that data.
- **NAS** Network Attached Storage (NAS) is a file-level storage architecture that makes stored data more accessible to networked devices.
- **Backup Media** – Any storage devices that are used to maintain data for backup purposes.
  These are often magnetic tapes, CDs, DVDs, hard drives, NAS Storage, or backup appliances
- **Restoration** – Also called "recovery." The process of restoring the data from its backup-up state to its normal state so that it can be used and accessed in a regular manner.

## 2.0 Purpose:

The purpose of backup policies is to ensure that there is a consistent and reliable method for recovering data.

## 3.0 Backup Policy

A backup policy is similar to an insurance policy - it provides the last line of defense against data loss and is sometimes the only way to recover from a hardware failure, data corruption, or a security incident.

The purpose of this policy is to provide a consistent framework to apply to the backup process. The procedure will provide specific information to ensure backups are available and useful when needed - whether to simply recover a specific file or when a larger-scale recovery effort is needed.

## 1. تعاریف

- **بک اپ:** برای کاپی کردن دیتا ها در ذخیره گاه دومی، صرفاً به منظور حفظ مصون دیتا ها استفاده میگردد.
- **NAS**: یک ساختار مشخص برای ذخیره سازی فایل است که دیتا های ذخیره شده را برای استفاده کننده های شبکه قابل دسترسی تر میسازد.
- **وسیله بک اپ:** هر وسیله ذخیره سازی که برای نگهداری دیتا ها برای اهداف بک اپ استفاده می شود.
- بازگردانیدن دیتا: پروسه بازیابی اطلاعات از بک اپ آن که حالت عادی خود را داشته باشد تا بتوانیم به طور منظم از آن استفاده کرد و به آن دسترسی داشت.

## 2. هدف:

3

هدف از رهنمود بک اپ گیری اطمینان از وجود یک روش سازگار و قابل اعتماد برای بازیابی معلومات است.

## 3. پالیسی بک اپ:

پالیسی بک اپ مشابه به یک بیمه است - آخرین خط دفاعی را در برابر از دست دادن دیتا ها ارائه می دهد و گاهی اوقات تنها راه برای بازیابی از خرابی سخت افزار، خرابی دیتا ها یا یک حادثه امنیتی است. که به منظور حفاظت و استفاده دوباره دیتا از آن استفاده میگردد.

7

هدف از این پالیسی ارائه یک چارچوب سازگار برای اعمال در پروسه بک اپ گیری است.

این روش اطلاعات خاصی را برای اطمینان از در دسترس بودن و مفید بودن بک اپ گیری در صورت نیاز ارائه میکند - چی صرفاً یک فایل خاص را بازیابی کنید یا زمانی که تلاش برای بازیابی در مقیاس بزرگتر مورد نیاز باشد.

این پالیسی برای تمام دیتا های ذخیره شده در سیستم ها قابل تطبیق میباشد.

این روش شامل مواردی مانند نوع دیتاهای است که باید بک اپ شوند، تعداد دفعات بک اپ، ذخیره‌سازی نسخه‌های بک اپ و روش‌های بازیابی دیتا.

## Table of Contents

This policy applies to all data stored on Board systems. The procedure covers such specifics as the type of data to be backed up, frequency of backups, storage of backups, retention of backups, and restoration procedures.

## 4.0 Procedure

### 4.1 Identification of Critical Data

The user must identify what data is most critical for MUDL. This can be done through an informal review of information assets in their computers. critical data should be identified so that it can be given the highest priority during the backup process.

### 4.2 Data to be Backed Up

A backup policy must balance the importance of the data to be backed up with the burden such backups place on the users, network resources, and the backup servers.
Data to be backed up will include:

- All data determined to be critical by the employee (employee job function data).
- stored data to local hard drives of desktops and laptops (It is the user's responsibility to ensure any important data is moved to the file server) OR ICT directorate responsibility to quarterly copy backup.

### 4.3 Data Not to be Backed Up

ICT Directorate will be not responsible for backing up data will include:

- User's personal data

## 4. روش بک اپ:

4,5,8

### 4.1 شناسایی دیتا های مهم و حیاتی

استفاده کننده باید تشخیص دهد که کدام دیتا ها برای وزارت مهم و حیاتی هستند . این را می توان از طریق بررسی غیررسمی دارایی های اطلاعاتی در کمپیوتر های خویش انجام دهند .دیتا های حیاتی باید شناسایی شوند تا بتوان در پروسه بک اپ گیری به آن ها اولویت داده شود.

### 4.2 دیتا های قابل بک اپ:

پالیسی بک اپ گیری اهمیت دیتا هایی که باید بک اپ شوند با مسولیت های که بر دوش کاربران، منابع شبکه و سرورها وارد می کند تعادل ایجاد کند.
دیتا های که بک اپ شوند شامل:

- تمام دیتا های که توسط کارمند برای بک اپ مشخص شده است (دیتا های مطابق به وظایف کاری کارکنان).
- دیتا های ذخیره شده در هارد دیسک های کمپیوتر های دسکتاپ و لپ تاپ (این مسئولیت استفاده کننده است که از انتقال دیتا های مهم به فایل سرور ریاست آی تی اطمینان حاصل کند) و یا ریاست تکنالوژی اطلاعاتی و ارتباطی مسئولیت کپی کردن دیتا های مشخص شده توسط کارمند را در هر سه ماه دارد.

### 4.3 دیتا های غیر قابل بک اپ:

ریاست تکنالوژی اطلاعاتی و ارتباطی مسئولیت در قبال بک اپ گیری از دیتا های را نخواهد داشت که شامل موارد ذیل می شوند:

- دیتا های شخصی کارمندان
- دیتا های موجود در ذخیره گاه های قابل انتقال ( سی دی، فلش میموری و ...)

- Data on removable media (i.e DVD's, CDs, and Thumb Drives)
- Data stored on mobile devices

## 4.4 Backup Storage

Storage of backups is a serious issue and one that requires careful consideration. Since backups contain critical, and often confidential Board data, precautions must be taken that are commensurate to the type of data being stored.
1 year of data will be kept on ICT- NAS.

## 4.5 Restoration Procedures and Documentation

The data restoration procedures must be tested and documented. Documentation should include exactly who is responsible for the restore, how it is performed and how long it should take from request to restoration.

- دیتا هاس موجود در مبایل ها.

## 4.4 ذخیره سازی بک اپ:

ذخیره سازی بک اپ یک مسئله جدی است و نیاز به بررسی دقیق دارد. از آنجایی که بک اپ حاوی دیتا های مهم و اغلب محرمانه وزارت هستند، باید اقدامات احتیاطی متناسب با نوع دیتا های ذخیره شده انجام شود.

دیتا های یک ساله اداره در ذخیره گاه ریاست تکنالوژی اطلاعاتی و ارتباطی موجود خواهند بود.

## 4.5 مراحل بازگرداندن دیتا و مسنتد سازی:

بازیابی دیتا ها باید آزمایش و مستند شوند.
فورم از قبل آماده شده درخواست بک اپ توسط شعبه نیازمند خانه پری شده و بعد از تائید توسط رئیس مربوطه به ریاست تکنالوژی ارسال میگردد. اسناد باید دقیقاً شامل اینکه چه کسی مسئول بازیابی است، چگونه انجام می شود و چه مدت از درخواست تا بازیابی باید طول بکشد.

Note: For any sentence accuracy please refer to English section.

ترتیب کننده
ریاست تکنالوژی اطلاعاتی و ارتباطی

ملاحظه شد
معینیت مالی و اداری

منظور کننده
مقام وزارت