ICT Rules for Y2024

SPS Updated : 25 Mar 2024

ICT Rules for Y2024 Rev. 01

Rule #1: 5ส File Server
Dynamic Data: Drive O:\, R:\, L:\
Static Data: Drive T:\, U:\
Disk Quota: TBA by SPS

Rule #4: VPN/WFH
Policy: Disable all VPN users
Approval Path:
User > Sup. > Mgr. > Director

Rule #2: USB Storage
Policy: Disable all USB Storage
Approval Path:
User > Sup. > Mgr. > ICT Mgr.

Rule #5: NCR-WiFi
Policy: Change Password every 180 days
NCR-WeCan: NCR Team Only
NCR-Learning: NCR Guest
(Customer, Supplier, Others)

Rule #3: User's Password
Policy: 8 Characters [Digit + Uppercase + Lowercase + Special Character]
Notes: Force a Group Policy by Server Manager, Password Expiration for Users

ติดตามอ่านรายละเอียดเพิ่มเติมจาก e-mail SPS เร็ว ๆ นี้ครับ

NCR The Hose Specialist.

ICT Rules for Y2024

Rule #1: 5ส File Server

Dynamic Data: Drive O:\, R:\, L:\
Static Data: Drive T:\, U:\
Disk Quota: TBA by SPS

Work Instructions:

1. Mgr. กำหนดรูปแบบ folder path ให้สอดคล้องกับ dynamic/static data
2. User ทำ 5ส file server [move static data from O:\ to T:\, R:\ to U:\ ]
3. SPS ตรวจสอบความสอดคล้องของ dynamic/static data
4. SPS แจ้ง disk quota และจัดทำ disk quota configuration (@Windows Policy)

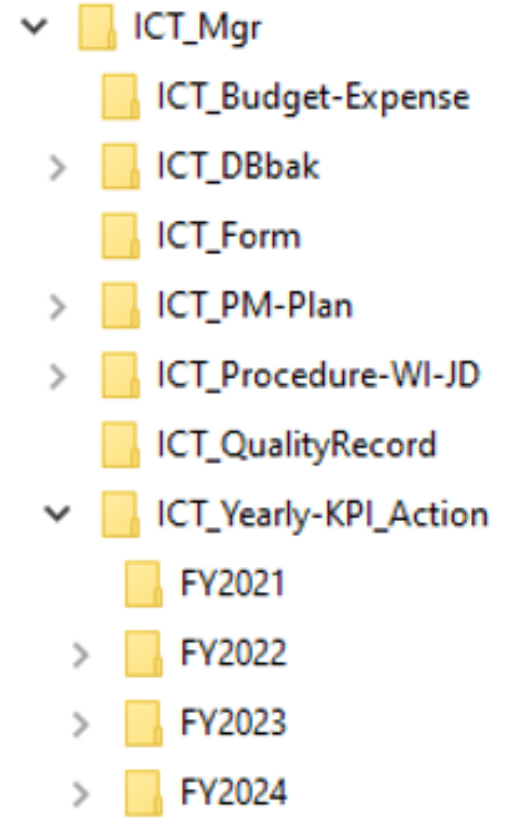
Notes:

Dynamic Data: Information that is vague, fleeting, free floating and ever changing.
Static Data: Information that is concrete, constant and stays the same.

Backup rules:

Dynamic Data: Daily > Monthly > Yearly
Static Data: Monthly > Yearly

ตัวอย่าง:
การจัด Folder/Subfolder
R:\ICT\ICT_Mgr\



Target: within 12 Apr 2024

The Hose Specialist.

ICT Rules for Y2024

Rule #2: USB Storage

Policy: Disable all USB Storage

Approval Path: User > Sup. > Mgr. > ICT Mgr.

Work Instructions:

1. ฝ่าย ICT ขอสงวนสิทธิ์ยกเลิก USB Storage ทุก users ที่อนุมัติก่อน Dec 2023
2. ฝ่าย ICT ดำเนินการ disable USB Storages [using Windows Group Policy/Client configuration]
3. การขออนุมัติใช้งาน USB Storage ปี 2024 ให้เป็นไปตาม approval path ข้างต้น
4. Users ผู้ได้รับอนุมัติสิทธิ์ใช้งาน USB Storage จะต้องปรับแผน P2A เป็น 2 ครั้ง/ปี

Notes:

Risks might include:

- Passing a virus or malware between machines.
- Data falling into the wrong hands simply by losing the device.
- Targeted hacking could be in the form of 'found' USB devices.

Status: Completed on 01 Feb 2024

ICT Rules for Y2024

Rule #3: User's Password

Policy: 8 Characters [Digit + Uppercase + Lowercase + Special Character]

Notes: Force a Group Policy by Server Manager, Password Expiration for Users

Work Instructions:

1. ฝ่าย ICT Force a Group Policy by Server Manager: มีผลบังคับใช้ password ใหม่ 01 Apr 2024
2. Users ต้องกำหนด password ให้สอดคล้องกับ password policy ข้างต้น
3. Password Expiration for Users : 180 days
4. ห้าม users แจ้ง username และ password ของตนเองให้บุคคลอื่นทราบโดยเด็ดขาด

Caution:

Risks associated with weak passwords

- Unauthorized access [การเข้าสู่ระบบและใช้คอมพิวเตอร์โดยไม่ได้รับอนุญาต]
- Account takeover
- Data breaches [การที่ข้อมูลถูกเข้าถึงโดยไม่ได้รับอนุญาต]
- Identity theft [การขโมยข้อมูลส่วนบุคคล]
- Financial losses

ICT Rules for Y2024

Rule #4: VPN/WFH

Policy: Disable all VPN users

Approval Path: User > Sup. > Mgr. > Director

Work Instructions:

1. ฝ่าย ICT ขอสงวนสิทธิ์ยกเลิก VPN users ทุก users ที่อนุมัติก่อนปี 2024
2. การขออนุมัติใช้งาน VPN ปี 2024 ให้เป็นไปตาม approval path ข้างต้น
3. ฝ่าย ICT จะทำการ reset VPN password ทุก ๆ ~~90 วัน~~ 180 วัน
4. Users ผู้ได้รับอนุมัติสิทธิ์ VPN ต้องส่ง laptop เพื่อทำ PM ที่ฝ่าย ICT ทุก ๆ 90 วัน

Notes:

When you use a VPN, you are still at risk of:

- Trojans
- Bots
- Malware (Ransomware)
- Spyware
- Viruses

ICT Rules for Y2024

Rule #5: NCR-WiFi

Policy: Change Password every 180 days
NCR-WeCan: NCR Team Only
NCR-Learning: NCR Guest (Customer, Supplier, Others)

Work Instructions:

1. ฝ่าย ICT จะทำการเปลี่ยน password สำหรับ WiFi NCR-WeCan ทุก ๆ 180 วัน
2. WiFi NCR-WeCan ใช้สำหรับพนักงาน NCR เท่านั้น
3. WiFi NCR-Learning ใช้สำหรับ mobile phone, self learning และ NCR Guest (Customer, Supplier, Others)
4. ห้าม users แจ้ง password WiFi NCR-WeCan ให้บุคคลภายนอกทราบโดยเด็ดขาด

Notes:

Security risks of public WiFi

- "Evil twin" attack [hacker จะตั้ง Hotspot AP (access point) ขึ้นมาแล้วปลอมตัวให้เหมือนกับเป็น AP]
- Man-in-the-middle attack (MitM). [ดักฟังบนเครือข่าย เพื่อรับข้อมูลการติดต่อธุรกรรม]
- Password cracking attack
- Packet sniffing attack [การเข้าถึงข้อมูลที่สำคัญ และดำเนินการเปลี่ยนแปลงข้อมูลนั้น]
- Security misconfigurations [การโจมตีความผิดพลาด จากการตั้งค่าส่วนต่าง ๆ ของระบบ]

NCR
The Hose Specialist.

Thank You

The Hose Specialist.