Cognizant
Passion for building stronger businesses

Cognizant Technology Solutions
Saudi Arabia Limited

كوجنيزانت تكنولوجي سوليوشنز
السعودية المحدودة

Introduction

مقدمة

Security responsibilities of the Associate are addressed during the recruitment stage. These are documented in the Non-disclosure, H1 and L1 Agreements, which are signed by the Associate during the joining process. The disciplinary action, which may be taken against violation of security requirements, is also mentioned.

تمت معالجة المسؤوليات الأمنية للزميل خلال مرحلة التوظيف. تم قيد تلك المسؤوليات في اتفاقيات عدم الكشف واتفاقيات اتش 1 وال 1 التي يتم توقيعها من قبل الزميل خلال عملية الانضمام. تم ذكر أيضاً الإجراء التأديبي الذي قد يتم اتخاذه ضد الإخلال بالمتطلبات الأمنية.

Including security in job responsibilities

ضم الأمن لمسؤوليات العمل

All Associates of Cognizant shall adhere to the Organization Security Policy. The various dimensions covered in the Security Policy at Cognizant include Physical Security, Logical Security, Network Security, Desktop Security and Anti-virus Security. It is mandatory for Associates to comply with all these dimensions of security as mentioned below:

يجب على كافة الزملاء في كوجنيزانت الالتزام بالسياسة الأمنية للشركة. التي تشمل الأبعاد المختلفة التي تمت تغطيتها في السياسة الأمنية لشركة كوجنيزانت الأمن الحقيقي والأمن المنطقي وأمن الشبكات وأمن سطح المكتب وأمن مكافحة الفيروسات. الزملاء ملزمين بالالتزام بكافة هذه الأبعاد الأمنية كما هو مذكور أدناه:

Any electronic items like laptops, mobiles etc shall be declared before entering the facility.

يتم التصريح عن أية أجهزة الكترونية مثل الحواسيب المحمولة والهواتف المحمولة قبل الدخول إلى المنشأة.

Cognizant
Passion for building stronger businesses

No material shall leave the facility without approval from authorized personnel.	يجب ألا تخرج أية مادة من المنشأة دون الحصول على موافقة من الموظفين المفوضين.
Any vendor/customer shall be accompanied by an Associate within Cognizant premises.	يجب أن يقوم زميل بمرافقة أي بائع/عميل ضمن مقر كوجنيزانت.
Associates shall adhere to the defined security procedures for various operating systems and databases.	يجب على الزملاء الالتزام بالإجراءات الأمنية المحددة لمختلف أنظمة التشغيل وقواعد البيانات.
Associates shall not log on to non-business sites. This has been ensured through HTTP authentication and non-business filtering.	يجب على الزملاء عدم الدخول إلى المواقع غير الخاصة بالأعمال. يتم التحقق من هذا الأمر عبر اعتماد HTTP وتصفية المواقع غير الخاصة بالأعمال.
Desktop Policy shall be adhered to.	يجب الالتزام بسياسة سطح المكتب.
Cognizant Certified Screensaver and wall paper shall be used on the desktop.	يتم استخدام شاشة التوقف والخلفية المعتمدة لشركة كوجنيزانت على سطح المكتب.
Clear desk policy shall be followed.	يجب اتباع سياسة السطح النظيف.
Anti-virus software shall be regularly updated by the Associates.	يجب تحديث برنامج مكافحة الفيروسات بشكل دائم من قبل الزملاء.
Associates shall keep their password confidential and shall not jot-down their password and or store it as a	يجب على الزملاء الاحتفاظ بسرية كلمة السر الخاصة بهم وعدم كتابة كلمة السر على عجل أو تخزينها

macro.

بصيغة ماكرو.

All Associates shall ensure that confidential information is not disclosed through phone, mail etc. This is ensured by signing an NDA (Non-disclosure agreement) when an employee enters the company.

يجب على كافة الزملاء التأكد من عدم كشف المعلومات السرية عبر الهاتف والبريد وخلاف ذلك. يتم تأكيد هذا الأمر من خلال توقيع اتفاقية عدم الافصاح عندما ينضم أي موظف للشركة.

For privileged users, NDA covering additional terms & conditions shall be signed.

بالنسبة للمستخدمين أصحاب الامتيازات يتم توقيع اتفاقية عدم افصاح تغطي شروط وأحكام إضافية.

Disciplinary Process

العملية التأديبية

All employees should adhere to the Organization security policies. Any breach in the defined policies shall be considered as a serious violation and will be referred to the Senior Management Committee for appropriate disciplinary action.

يجب على كافة الموظفين الالتزام بالسياسات الأمنية للمؤسسة. يعتبر أي إخلال بالسياسات المحددة أنه إخلال خطير ويحال إلى لجنة الإدارة الأولى لاتخاذ الإجراء التأديبي المناسب.

Cognizant
Passion for building stronger businesses

DEFAULT USER RIGHTS ON COGNIZANT NETWORK

حقوق المستخدم الافتراضية على شبكة كوجنيزانت

The high level guidelines for implementing desktop policy are outlined as follows. The associate is required to go through the below mentioned points and sign the rights document failing which a user id will not be provided:

فيما يلي أدناه إرشادات التطبيق عالية المستوى لسياسة سطح المكتب. يجب على الزميل الاطلاع على النقاط المذكورة أدناه وتوقيع مستند الحقوق وإلا لن يتم تقديم هوية مستخدم:

Physical Access:

الدخول الفعلي:

Associates shall not be allowed to open or move the Computer System, for any reason.

لا يسمح للزملاء بفتح أو نقل نظام الحاسوب لأي سبب كان.

Desktop BIOS settings:

إعدادات بيوس سطح المكتب:

• BIOS Setup Password:

• كلمة سر إعداد البيوس:

The BIOS Setup password shall be enforced on all desktop and only known to NSS personnel.

تطبق كلمة سر إعداد البيوس على كافة أجهزة الحاسوب وتكون معروفة لموظفي خدمة أمن الشبكات.

• Power On /Boot Password:

• كلمة سر التشغيل/الإقلاع:

The Power-on password shall be enforced on all desktops. This will serve as a first level access security for the desktops.

يجب استخدام كلمة سر التشغيل في جميع أسطح المكتب. هذا الأمر يعتبر إجراء أمني للدخول من المستوى الأول لأسطح المكتب.

• **Booting process:**

Booting from active devices like CD-ROM, Floppy Drive, Boot ROM etc. shall be disabled.

• **عملية الإقلاع:**

يتم تعطيل الإقلاع من أجهزة فعالة مثل سواقة الأقراص المضغوطة وسواقة الأقراص المرنة وسواقة الإقلاع وخلاف ذلك.

User Level Access Rights:

• The Associate shall not be a part of the local Administrators/Power Users group. Administrator access shall be removed from the desktop so that the Associate cannot install any software or make any changes to the system settings.

• Associates shall not be permitted to share any folders in their machines.

• Associates shall be advised not to download technical literature / white papers, shareware / freeware software tools etc. from the Internet.

• Associates shall not be allowed to change the basic settings like default IP Address, Service Pack, System Partition, and Default Services etc.

حقوق الدخول إلى مستوى المستخدم:

• لن يكون الزميل جزءً من مجموعة الإداريين المحليين/مستخدمي الطاقة المحليين. يتم حذف دخول الإداري من سطح المكتب بحيث لا يكون باستطاعة الزميل تركيب أي برنامج أو إجراء أية تغييرات على إعدادات النظام.

• لا يسمح للزملاء بمشاركة أية مجلدات في أجهزتهم.

• يتم إبلاغ الزملاء بعدم تحميل النشرات الفنية والمستندات التقنية وبرامج المشاركة/البرامج المجانية أو خلاف ذلك من الانترنت.

• لا يسمح للزملاء بتغيير الإعدادات الأساسية مثل عنوان بروتوكول الانترنت وحزمة الخدمة وتقسيم النظام والخدمات الافتراضية وخلاف ذلك.

Standard Wallpaper & Screen

تطبيق الخلفية وشاشة التوقف

Cognizant
Passion for building stronger businesses

Saver Implementation:

The standard wallpaper & screen saver [designed by Cognizant] shall be enabled with password protection and an idle timeout of 5 minutes, to prevent unauthorized access.

الموحدة:

يـتم تطبيـق خلفيـة وشاشـة توقـف موحـدة [مصـممة مـن قبـل كوجنيزانـت] مـع حمايـة بكلمـة سـر وزمـن انتظـار يبلـغ 5 دقائق لمنع الدخول غير المصرح به.

Operating System Level Security:

To avoid any misuse or unauthorized access, the following OS level restrictions shall be implemented by changing the appropriate registry values:

مستوى أمن نظام التشغيل:

لتفـادي أي سـوء اسـتخدام أو دخـول غيـر مصـرح بـه يـتم تطبيـق قيـود مسـتوى نظـام التشـغيل التاليـة مـن خـلال تغييـر قيم التسجيل المناسبة :

• Issuance of Anonymous User Accounts shall be restricted.

• يمنـع إصـدار حسـابات مسـتخدم دون مسمى.

• Only Administrators shall be allowed to change/configure NT Base objects such as files, printers and processes.

• يسـمح فقـط للإداريـين بتغيير/إعـداد مـواد قاعـدة ان تـي مثـل الملفـات والطابعات والعمليات.

• Only Associates having valid user ID & password shall be allowed to log on to the system.

• يسمح فقط للزملاء الذين يكون لديهم هويـة مسـتخدم وكلمـة سـر سـارية بالدخول إلى النظام.

• Automatic Logon shall be disabled.

• يتم تعطيل الدخول الآلي.

• Caching of logon credentials shall be disabled.

• يـتم تعطيـل التخـزين المؤقـت لمعلومـات تسجيل الدخول.

• Names of previously logged-on users shall not be displayed in order to protect the secrecy of user names.

• يجب عدم عرض أسماء المستخدمين الذين قاموا بتسجيل الدخول سابقاً لحماية سرية أسماء المستخدمين.

• Only Administrators shall be allowed to use the scheduler service with the AT Command.

• يسمح فقط للإداريين باستخدام خدمة المجدول من خلال أمر ايه تي.

• The NT Page file shall be cleared on system shutdown to prevent a publicized attack to use any information saved on the paging file.

• يتم مسح ملف صفحة ان تي عند إيقاف تشغيل النظام لمنع أي هجوم معلن لاستخدام أية معلومات محفوظة في ملف التصفح.

Protecting Floppies and CD-ROM Drives:

حماية الأقراص المرنة وسواقات الأقراص المضغوطة:

Access to floppy disk or CD-ROM Drive shall be restricted to authorized users only.

ينحصر الدخول إلى سواقة القرص المرن أو القرص المضغوط بالمستخدمين المصرح لهم فقط.

Remote Access Services:

خدمات الدخول عن بعد:

• Remote Access Services & Dial In Modem port shall be disabled to avoid any possibility of remote access to the desktop from the network.

• يتم تعطيل خدمات الدخول عن بعد ومنفذ مودم الاتصال لتفادي أية إمكانية للدخول عن بعد إلى سطح المكتب من الشبكة.

• Remote access tools like PCAnywhere, VNC, Damewhere etc. shall not be installed on the desktops.

• يجب عدم تركيب أدوات الدخول عن بعد مثل PCAnywhere, VNC, Damewhere أو خلاف ذلك على أسطح

المكتب.

حصر عملية إيقاف التشغيل:

يمكن فقط للمستخدم والإداريين الذين قاموا بتسجيل الدخول حالياً إيقاف تشغيل أية محطة عمل.

Restricted Access for Shutdown:

Only the currently logged-in user and Administrators can shut down a workstation.

الاطلاع على السجل عن بعد:

ينحصر الاطلاع على أي سجل محطة عمل بالإداريين فقط.

Remote Registry Access:

Remote access to a workstation registry shall be restricted to Administrators only.

إعدادات المنطقة الآمنة لبرنامج انترنت اكسبلورر:

يتم تطبيق حزمة التعديل الأمني لبرنامج انترنت اكسبلورر التي تضع مستويات أمن محسنة لكافة المناطق الآمنة ولا تسمح للمستخدمين بتغيير هذه الإعدادات.

Internet Explorer Security Zone Settings:

The IE Security Customization Package, which sets optimized security levels for all security zones and disables users from changing these settings, shall be implemented.

مكافحة الفيروسات:

يجب تركيب برنامج لمكافحة الفيروسات على كافة أسطح المكتب كإجراء طبيعي ويتم تحديثه آلياً بشكل مستمر.

Anti Virus:

Anti-virus software shall be installed on all desktops by default and updated automatically on a regular basis.

رسالة تسجيل الدخول ورسالة الترحيب والإعلانات:

Logon Message, Welcome Message and Announcements:

Cognizant
Passion for building stronger businesses

The logon and welcome messages shall not contain any information that could aid unauthorized persons in gaining access to the system.

يجب ألا تتضمن رسائل تسجيل الدخول والترحيب أية معلومات قد تساعد أشخاص غير مصرح لهم على الدخول إلى النظام.

Signature of the associate: **توقيع الزميل:**

Date: **التاريخ:**