

Security Access /Internet Permissions Form

Section 1. Contact Information		(NAME IN BLOCK LETTERS ONLY)
College or Department or Company :		
User Full Name :		
Mobile:	Email :	
Tel:	Extension:	ITSM NO :
Date :	Saudi / IQAMA ID :	

Section 2.0 Specific Access System / Server					
Source (From) System /Server	Destination (To) System / Server	Protocol	Port no	Direction	Remarks
		TCP		Unidirectional ☐ Bidirectional ☐	
		TCP		Unidirectional ☐ Bidirectional ☐	
Access period :			Request type : New ☐ Renewal ☐		
Access Timings :			Risk Factor Risk ☐ No Risk ☐		

Section 2.1 Reason for Server Access in detail.

Requestor Department Dean / Vice Dean /Manager		
☐ Approval ☐ Reject ☐ request info	Name	Signature

Internal use - Deanship of Information Technology - Dean / Vice Dean Approval		
☐ Approval ☐ Reject ☐ request info	Name	Signature

Internal use - Deanship of Information Technology - Engineer	
Engineer Name	Signature

1. Network security support policies

- 1.1. The department will provide the client/users with highly secured network & IP address to communicate with other internal and public network as per required situation.
- 1.2. The department will open only secured ports on firewall for any communication within local & public network for all the servers.
- 1.3. The standard facilities will only be provided to clients/pc/laptop & servers which are joined to NBU domain.
- 1.4. All the clients/PC's/laptops and servers should be added to the NBU domain. Any PC/server not added to the NBU domain will be disconnected from the network and the department will not be responsible for this action.
- 1.5. All the departments should keep the data back-up for their Servers. In case of any hardware/media failure of the servers, network department will not be responsible for the lost data.
- 1.6. All the department are requested to secure the servers credentials with a strong passport that should be minimum 8 characters including capital & small letters, numbers and symbol.

2. Internet Use Filtering System

The Information Technology Department shall block access to Internet websites and protocols that are deemed inappropriate for NBU's environment. The following protocols and categories of websites should be blocked.

- o Advertisements & Pop-Ups
- o Chat and Instant Messaging
- o Adult/Sexually Explicit Material
- o Gambling
- o Hacking
- o Illegal Drugs
- o Intimate Apparel and Swimwear
- o Peer to Peer File Sharing
- o Personals and Dating
- o Social Network Services
- o SPAM, Phishing and Fraud
- o Spyware
- o Tasteless and Offensive Content
- o Violence, Intolerance and Hate
- o Web Based Email

☐ I agree with the terms and conditions stated in the request form.

Name:	_____
Job Title:	_____
Signature:	_____
STAMP	_____

1. سياسات دعم أمن الشبكة:

- 1.1. سوف يوفر القسم للمستخدمين شبكة عالية الحماية سواء كانت شبكات داخلية أو شبكات عمومية.
- 1.2. فتح المنافذ المحمية فقط في جدار الحماية لأي اتصال داخلي أو خارجي.
- 1.3. توفير خدمة استخدام الشبكة للأجهزة (المكتبية - المحمول - الخوادم) التابعة لإدارات الجامعة والمضافة للمجال فقط.
- 1.4. الحرص على إضافة جميع الأجهزة الموجودة داخل شبكة الجامعة إلى المجال الخاص بشبكة الجامعة وأي جهاز لم يتم إضافته للمجال سوف يتم فصل الشبكة عنه ولن تكون إدارة الشؤون الفنية مسؤولة عن هذا الإجراء.
- 1.5. على جميع الإدارات المسؤولة عن خوادم ملزمة بعمل نسخ احتياطي لكل خادم وفي حال تعرض الخوادم لأي مشكلة بدون اتخاذ الإجراء اللازم لعمل النسخ الاحتياطي لن تكون إدارة الشؤون الفنية مسؤولة عن هذه البيانات.
- 1.6. جميع الأقسام ملزمة بالاحتفاظ ببيانات المصادقة الخاصة بالأنظمة والخوادم (username and password) وعدم إفشاء هذه البيانات للأشخاص الغير مخولين باستخدام الخوادم واستخدام كلمة مرور تحتوي على 8 خانات كحد أدنى متضمنة حروف، رموز وأرقام.

2. نظام فرز استخدام مواقع شبكة الانترنت:

يتوجب على عمادة تقنية المعلومات حجب ومنع الوصول لمواقع الانترنت الغير متلائمة مع بيئة الجامعة، وسوف يتم حظر البروتوكولات الخاصة بالمواقع التالية:

- o الإعلانات والإطارات المنبثقة.
- o مواقع وبرامج المحادثات والمراسلات السريعة.
- o المواقع التي تحتوي على مواد جنسية إباحية.
- o المواقع الخاصة بالمقامرة.
- o المواقع التي تحتوي على مواد و أدوات الاختراق والتهكير.
- o مواقع وبرامج التحميل السريع.
- o مواقع وبرامج التواصل الاجتماعي.
- o مواقع وبرامج التجسس.
- o المواقع التي تقوم بإرسال بريد يحتوي على روابط الفش والاحتيال.
- o المواقع التي تحت على التعصب والعنف السياسي.

☐ أنا موافق على الشروط والاحكام الواردة في نموذج الطلب

الاسم:	_____
الوظيفة:	_____
التوقيع:	_____