افغانستان اسلامي امارت

لوړو زده کړو وزارت

تابش پوهنتون

اداري او مالي چارو معاونيت

معلوماتي تکنالوژۍ آمريت

معلوماتي تکنالوژۍ د اسانتياوو د ساتنې، پاملرنې او مناسبې استفادې پاليسي

کال: ۱۴۰۵


بسم الله الرحمن الرحیم

فهرست

معلوماتي تکنالوژۍ پالیسي (لارښود)

اوله ماده: د پالیسۍ پیژندنه

تابش پوهنتون چې د لوړو زده کړو وزارت د چتر لاندې خپل اداري او علمي فعالیتونه پر مخ وړي، چې پدې لړ کې یې د لوړو زده کړو وزارت، ملي او نړیوالو معیارونو په نظر کې نیولو سره د نوي عصر او پر تکنالوژۍ د سمبال اداري او علمي چاپیریال په رامینځته کولو کې تل زیار او کوښښ کړی او پدې برخه کې د لازیاتو پرمختګونو او نوو سیستمونو په ایجاد او انکشاف باندې کار جریان لري، پوهنتون د نوي عصر او تکنالوژۍ د کارونې جامع او پرمختللي سیستمونه رامینځته کړي، چې د یادو سیستمونو څخه د استادانو، اداري کارمندانو او محصلینو د موثرې ګټې اخیستنې په موخه د پوهنتون په کچه د اداري او مالي چارو معاونیت په تشکیل کې د معلوماتي تکنالوژۍ آمریت ایجادکړی، تر څو د یوې منظمې پالیسۍ مطابق د پوهنتون د تخنیکي، انترنیټي، کمپیوټرنو، ویبسایټونو، ډیټابیسونو، شبکو، معلوماتي سیستمونو ته د لاسرسي، د اکاونټونو بندولو او محدودولو د معلوماتو محرمیت او سرغړونو لپاره د څارنې او نظارت په برخه کې د معلوماتي تکنالوژۍ آمریت لپاره دا پالیسي ترتیب شوه، دا پالیسي د لارښوونو او مقرراتو یوه ټولګه ده چې په اداره کې د معلوماتي تکنالوژۍ سرچینو خوندي او مسؤلانه کارونه ډاډمنه کړي، دا پالیسي هغه اصول، معیارونه او طرز العملونه په ګوته کوي چې د پوهنتون لخوا چمتو شوي تر څو د تکنالوژۍ سیستمونو، شبکو او خدماتو مناسبه او اصولي اداره کول یقیني کړي.

معلوماتي تکنالوژۍ آمریت هغه مهم اصل او رول پیژني چې د تیکنالوژۍ په مرسته د ټولنې او همدارنګه د پوهنتون د اکاډمیکو، اداري او څیړنیزو فعالیتونو په لړ کې لوبوي، مور هڅه کوو چې یوخوندي، د باور وړ او ټول شموله ډیجیتل اداري او علمي چاپیریال او سیستمونه رامینځته کړو چې د پوهنتون د ستراتیژیکو موخو، لړلید او ماموریت، نوښت، همکارۍ او غوره والي ته وده ورکړي.

پالیسي به په دوره یي توګه نوی او تازه کیږي او بیا کتنه به یې ترسره کیږي تر څو د پرمختللې تکنالوژۍ سره مطابقت منعکس کړي او راپورته کیدونکو ننګونو ته ځواب ووایی دا زمونږ د پوهنتون د هر غړي مسولیت دی چې ځان له دې پالیسۍ سره اشنا کړي، ددې احکامو او لارښوونو پابند وي، او د هرې سرغړونې یا اندیښنې په رابطه اړونده مسؤلو اشخاصو ته راپور ورکړي.

ددې پالیسۍ کې د بیان شوي اصولو په ساتلو سره مونږ کولي شو یو خوندي، خوځنده او ټول شموله چاپیریال رامینځته کړو او وده ورکړواو همدارنګه د لوړو زده کړو لپاره د وزارت د تضمین کیفیت او نورو معیارونو د پوره کولو لپاره جامع او هر اړخیزه چوکاټ او تعقیب رامینځته کړو، پالیسي د ټولو اړخونو په نظر کې نیولو سره په (۲۸) مادوکې ترتیب شوه.

دویمه ماده: د پالیسۍ هدف

د تابش پوهنتون د معلوماتي تکنالوژۍ پالیسۍ موخه د پوهنتون د ټولو غړو (استادانو، اداري کارکوونکو، محصلینو او مجاز میلمنو) په ګډون د معلوماتي تکنالوژۍ د سرچینو او سیستمونو د کارولو لپاره د اصولو، لارښوونو او توقعاتو توضیح کول دي، د پالیسۍ هدف د خوندي، باوري، نوښت، ابتکار او انکشاف په برخه کې د ډیجیتل او کمپیوټري اداري او علمي چاپیریال رامینځته کول او وده ورکول دي تر څو د پوهنتون د تحصیلي، څیړنیزو لیدلورو او ماموریتونو ملاتړ وکړي.

1.2. امنیت: د پوهنتون د معلوماتي تکنالوژۍ پالیسي یو له لومړنیو هدفونو څخه د پوهنتون د ډیجیتل شتمنیو او سیستمونو امنیت تضمین کول دي، په دې کې ممکن د حساسو معلوماتو، څیړنیزو موادو، فکري ملکیت، اود استادانو، کارمندانو او

محصلینو د شخصي معلومات شامل وي، پالیسي ممکن د غیر مجاز لاسرسي، ډیټا سرغړونو، او سایبر ګواښونو په وړاندې د ساتنې لپاره امنیتي اقدامات لکه د اور وژنې، انټي ویروس سافټویرونه، کوډ کول او د خوندي شبکې لپاره د اړونده اقداماتو او سیستمونو ډاډ ورکوي.

2.2. د معلوماتو محرمیت او اطاعت: پالیسي به د معلوماتو محرمیت په اهمیت باندې ټینګار وکړي او د اړوندو قوانینو او مقرراتو سره مطابقت یقیني کړي، لکه د عمومي معلوماتو محافظت مقررات (GDPR) یا د کورنۍ د تعلیمي او تحصیلي حقونو او محرمیت قانون (FERPA) ، دا ممکن د معلوماتو راټولولو، ذخیره کولو، کارولو، شریکولو، ساتلو او شخصي معلوماتو ته د لاسرسي او کنټرول لپاره د کارکوونکو او محصلینو د حقونو پورې اړونده ستونزې حل کړي.

3.2. مسؤله کارونه: د معلوماتي تکنالوژۍ پالیسي به د پوهنتون د معلوماتي سرچینو مسولانه او اخلاقي کارونې ته وده ورکړي، دا کیدای شي د منلو وړ کارونې طرز العملونه او لارښوونې تعریف کړي، په شمول د مناسب انلاین چلندونو لپآره لارښوونې، د غیر مجا لاسرسي یا سرچینو کارولو منع کول، او د فعالیتونو محدودیتونه لکه ځوروني، د کاپي حق څخه سرغړونه یا د ناوړه سافټویرونو په خپل سر نصبول.

4.2. د سرچینو تخصیص: پالیسي به په پوهنتون کې د معلوماتي تکنالوژۍ سرچینو تخصیص او مدیریت لپاره لارښوونې رامینځته کړي، پدې کې به ممکن د هارډویر، سافټویر، شبکې زیربنا او تدارک، ځای پرځای کول، ساتنه او د ځای پر ځای کولو او د کار په جریان کې د ستونزو حل کول شامل دي، او همدارنګه د سافټویر او یا هم د معلوماتي تکنالوژۍ په برخه کې د جواز ورکولو، بودیجې او د سرچینو د لومړیتوب لارښوونې شاملې دي.

5.2. ښوونه او روزنه: د معلوماتي تکنالوژۍ پالیسي د پوهنتون د کارکوونکو او محصلینو په منځ کې د معلوماتي تکنالوژۍ د امنیت، غوره او با مسؤلیته کړنو، د معلوماتو محرمیت او د سیستمونو او زیربناو په اړه پوهاوی رامینځته کوي، پدې کې روزنیز پروګرامونه، ورکشاپونه، او نورې مختلفې برنامې شاملې وي تر څو کارووونکو سره د احتمالي خطرونو په پوهیدو کې مرسته وکړي، او د دوي ډیجیتل پوهې ته وده ورکړي او د کمپیوتري او عصري نړۍ خوندي فعالیتونه ترسره او غوره کړي.

6.2. دوام او بیارغونه: دا پالیسي به د معلوماتي تکنالوژۍ د دوام او د ستونزو په صورت کې د بیا رغونې پلانونو ساتلو لپاره تګلارې په ګوته کړي تر څو ډاډ ترلاسه شي چې د (IT) مهم سیستمونه او خدمات د ګډوډۍ یا ناورین په صورت کې بیا رغول کیدای شي، پدې کې کیدای شي د بیک اپ پروسیجرونه، د معلوماتو د بیرته راګرځولو پروګرامونه او د (IT) پورې اړوند ساحو پر وړاندې دستونزو د اغیزو کمولو لپاره بیړني پلانونه او اقدامات شامل دي.

7.2. همکاري او نوښت: د معلوماتي تکنالوژۍ پالیسي به د ټیکنالوژۍ وسایلو، وسیلو، پلیټ فارمونو او سرچینو کارولو او هڅولو سره همکاري د نوښت کلتور ته وده ورکړي، چې د څیړنې، تدریس، زده کړې او اداري پروسو اسانتیاوې برابروي، دا به په پوهنتون کې د ډیجیتل بدلون لپاره د راپورته کیدونکي تکنالوژیکي نوښتونو او ابتکاراتو د ادغام او ملاتړي نوښتونو ته وده ورکړي.

8.2. موافقت: معلوماتي تکنالوژۍ پالیسي د اداري جوړښت، رول او د معلوماتي تکنالوژۍ آمریت او په پوهنتون کې د پریکړې کولو پروسې پورې اړوند مسؤلیتونه بیان او واضح کوي، دا ممکن د اړوندو قوانینو، مقرراتو او د لوړو زده کړو وزارت د معیارونو سره د مطابقت، او همدارنګه د داخلي پالیسیو او طرز العملونو تعقیب په نښه او تطبیق کړي.

دریمه ماده: د پالیسی د تطبیق ساحه

په تابش پوهنتون (ننګرها) کې د معلوماتي تکنالوژۍ پالیسۍ د تطبیق ساحه په عمومي ډول د لارښوونو، قواعدو، سیستمونو او کړنو پراخه لړۍ پوځي چې د پوهنتون په چاپیریال کې د معلوماتي تکنالوژۍ سرچینو او سیستمونو کارول اداره کوي، پالیسي ددې لپاره ډیزاین شوې چې د تکنالوژۍ موثره ، اغیزمنه او خوندي کارونه یقیني کړي، او د کارووونکو تر منځ د معلوماتي وسایلو او سیستمونو د کارونې په لړ کې مسؤلانه او اخلاقي چلند ته وده ورکړي، په لاندې ډول د معلوماتي تکنالوژۍ د تطبیق عمومي ساحات په نښه شوي:

د منلو وړ کارونه: پالیسي د معلوماتي تکنالوژۍ سرچینو او سیستمونو د منلو وړ کارونه په ګوته کوي، په شمول د کمپیوټر، شبکې، سافټویر، او ډاټا. دا ددې منابعو ټاکل شوي اهداف او د دوي په کارولو کې محدودیتونه مشخص کوي، لکه د غیر قانوني لاسرسي منع کول، غیر قانوني فعالیتونه یا ځوروني منع کول.

1.3. د منلو وړ کارول: پالیسي د معلوماتي ټکنالوژۍ سرچینو او سیسټمونو د منلو وړ کارول په ګوته کوي، په شمول د کمپیوټر، شبکې، سافټویر، او ډاټا. دا د دې منابعو ټاکل شوي اهداف او د دوی په کارولو کې کوم محدودیتونه مشخص کوي، لکه د غیرقانوني لاسرسي منع کول، غیرقانوني فعالیتونه، یا ځوروني.

2.3. شبکه او انټرنیټ: پالیسي د پوهنتون د شبکې او انټرنیټ اتصال کارول په ګوته کوي، په شمول د مسؤلیت او خوندي انټرنیټ لټون کولو لارښوونې، د برښنالیک کارولو، ټولنیزو رسنیو او صفحاتو او انلاین اړیکو لپاره د لارښوونو په برخه کې د کارونې وړ ده.

3.3. د معلوماتو امنیت او محرمیت: پالیسي د حساسو معلوماتو د ساتنې پر اهمیت ټینګار کوي او د ډیټا امنیتي تدابیر تعریفوي، لکه د پټنوم ساتنه، کوډ کول او د معلوماتو د بیک اپ پروسیجرونه دا ممکن د کارمندانو د شخصي معلوماتو پورې اړوند د محرمیت ساحې او د اړونده معلوماتو محافظت هم ډاډمن کړي.

4.3. سافټویر او جواز ورکول: پالیسي به د جواز لرونکي سافټویرونو کارول په ګوته کړي، پشمول د سافټویر جواز ورکولو ټرونونو سره د مناسب نصب، کارولو او اطاعت لپاره لارښوونې.

5.3. فکري ملکیت: پالیسي ممکن د فکري ملکیت حقوق ته د درناوي لپاره لارښوونې په ګوته کړي، په شمول د کاپي حق قوانین، په هغه صورت کې چې په پوهنتون کې د معلوماتي تکنالوژۍ سرچیني کاروي.

6.3. سایبر امنیت: په پالیسۍ کې ممکن د سایبر امنیت ګوابنونو پر وړاندې د ساتنې لپاره اقدامات شامل وي، لکه مالویر، فشینګ بریدونه، یا غیر مجاز لاسرسی. دا ممکن د انټي ویروس سافټویر، د سافټویرونو تازه کول او د کارووونکي د پوهاوي روزنې په برخه کې فعالیتونه او اړتیاوي په ګوته کړي.

7.3. د کارمندانو شخصي معلوماتي وسایل: په هغه صورت کې چې د تطبیق وړ وي د کارمندانو د شخصي وسایلو (BYOD) په برخه کې د شخصي وسایلو لکه لپټاپ، موبایل، ټابلیټونه یا نورو برخو کې لارښوونې چمتو کړي.

8.3. د کارووونکي مسؤلیتونه او چلند: پالیسي د معلوماتي تکنالوژۍ سرچینو د کارولو پر مهال د کارووونکو مسؤلیتونه او تمه شوی چلند تعریفوي، دا کیداي شي ستونزې لکه د غلا، ځوروني، غیر مجاز لاسرسي او د یادو مواردو د رامینځته کیدو پایلې تعریف کړي.

9.3. ډیټابیس او ویبسایټ: پالیسي به د پوهنتون د ډیټابس (ERP) سیستم او همدارنګه د ویبسایټ لپاره د قراردادونوترسره کولو، د معلوماتو اپډایټ ساتلو او د ډیټابیس او ویبسایټ په برخه کې کارکوونکو ته د هغوي د اړونده برخو د حقوقو ورکولو پروسیجرونه په ګوته کوي.

10.3. اطاعت او تطبیق: پالیسي د پالیسی سرغړونو د تحقیق او حل کولو طرز العملونه په ګوته کوي، په شمول د انضباطي کړنو او احتمالي قانوني پایلو په برخه کې.

څلورمه ماده: د پالیسی بیا کتنه

د معلوماتي تکنالوژی چټک پرمختګ او د معلوماتي سیستمونو پرمختللې چاپیریال د پالیسیو او لارښوونو دوره یي بیاکتنې ته اړتیا لري چې د دوي کارول اداره کوي، په پوهنتون کې د معلوماتي تکنالوژی بیا کتنه اړینه ده تر څو ډاډ ترلاسه شي چې پالیسي د اوسني عصري اداري سیستمونو او چاپیریال سره سمون لري، د پالیسی د بیا کتنې موخه د موجوده چوکاټ ارزونه، د ښه والي لپاره د ساحو په ګوته کول او د پوهنتون په چاپیریال کې د معلوماتي سرچینو موثریت، امنیت او مسؤلانه کارونې لپاره ضروري ده، د پالیسی د بیا کتنې موخه به دا وي چې ډاډ ترلاسه شي چې د معلوماتي تکنالوژی پالیسی اړونده، موارد جامع او د لوړو زده کړو وزارت او پوهنتون د اصولو نورو برخو سره د تطابق او د پوهنتون د لنډ مهاله او اوږد مهاله اهدافو سره سمون لري، په پایله کې د معلوماتي تکنالوژی پالیسی بیا کتنې (تجدید) موخه داده چې د پوهنتون د ماموریت ملاتړ وکړي د کاروونکو تجربې لوړې کړي او د تکنالوژی له پلوه مسلکي او خوندي اکاډمیک چاپیریال کې مرسته وکړي.

پنځمه ماده: کلیدي اصطلاحات او مخففات

No	Abbreviation	English	Pashto
1	IT	Information Technlogy	معلوماتي ټکنالوژي
2	GDPR	General Data Protection Regulation	د عمومي معلوماتو د ساتنې مقررات
3	FERPA	Family Educational Rights and Privacy Act	د کورنۍ تعلیمي حقونو او محرمیت قانون
4	Platforms	Software Or Hardware Systems	سافټویر یا هارډویر سیسټمونه
5	BYOD	Bring Your Own Device	د معلوماتي تکنالوژی شخصي وسایل
6	SLAs	Service Level Agreements	د خدماتو ترونونه
7	ITSM	IT Service Management	د معلوماتي ټکنالوجی خدماتو مدیریت
8	WCAG	Web Content Accessibility Guidelines	د ویب منځپانګې د لاسرسي لارښوونې
9	UPS	Uninterruptible Power Supply	د وقفې پرته د بریښنا رسول
10	PDUs	Power Distribution Units	د بریښنا د ویش واحدونه
11	SOPs	STandard Operating Procedures	معیاري عملیاتي پروسیجرونه
12	NVRs	Network Video Recorders	د شبکې ویډیو ریکارډر
13	VMS	video management software	د ویډیو مدیریت سافټویر
14	LMS	Learning Management System	د زده کړې مدیریت سیسټم
15	Bandwidth	Bits Per Second bps	په یوه ثانیه کې بیټس
16	Phishing	Form of cyber attack	د سایبر برید کولو یوه بڼه
17	Spamming	Sending Unsolicited and Unwanted Messages	د د ناغوښتل شوو پیغامونو لیږل
18	VPNs	Virtual Private Networks	انلاین خصوصي شبکې
19	ERP	Enterprise Resource Planning	د سرچینو پلان کول
20	Focal Person	Primary Contact or Representative	لومړنۍ اړیکه یا استازی
21	Scheme	Programming Language Scheme - URI Scheme	د پروګرام کولو ژبه
22	Algorithms	Set of step-by-step instructions or Procedures	د لارښوونو یا پروسیجرونو سیټ
23	CC	Carbon Copy	د کاربن کاپي
24	BCC	Blind Carbon Copy	پټه کاربن کاپي
25	PMS	Patch Management Systems	(د کمپیوترونو فعالیت ته وده ورکول)

26	Malware	Combination of words "malicious" and "software	ناوړه سافټویرونه
27	MDM	Mobile Device Management	د ګرځنده وسیلې مدیریت
28	MFA	Multi Factor Authentication	د څو فکتور تصدیق
29	Iris Scans	Biometric Technology	بایومتریک ټیکنالوژي
30	USB	Universal Serial Bus	د ډیټا ګړندی انتقال
31	Offsite	Storing Data, Resources In a Separate Location	د معلوماتو ذخیره کول، سرچینې په جلا ځای کې
32	Hotspot	Wireless Internet Connectivity	د بې سیمه انټرنیټ اتصال
33	Internet Traffic	Volume And Flow Of Data Transmitted Between Devices	د وسیلو تر مینځ لیږدول شوي ډیټا حجم او جریان
34	Linux	Open-Source Operating System	د خلاصې سرچینې عملیاتي سیستم
35	MacOS	Proprietary Operating System (Apple)	د ملکیت عملیاتي سیستم
36	Anti-Virus	Remove Malicious Software	د ناوړه سافټویرونو لرې کول
37	Flash Drive	Portable Storage Device	د ذخیره کولو وسیله
38	DHCP	Dynamic Host Configuration Protocol	د شبکې تنظیماتو لپاره کارول کیږي
39	Sensors	Detect and Measure Physical or Environmental Attributes	د فزیکي یا چاپیریالي خانګړتیاوې کشف او اندازه کړئ

شپږمه ماده: د پالیسی لارښود) عمومي اصول

تابش پوهنتون د معلوماتي تکنالوژی پالیسي د اداري کارکوونکو، استادانو او محصلینو لپاره د خوندي او ګټور کمپیوتري (ډیجیتل) چاپیریال رامینځته کولو او ساتلو اړین اصول وړاندې کوي، چې په لاندې ډول وړاندې کیږي:

1.5. د منلو وړ کارونه: په واضح ډول د پوهنتون د معلوماتي تکنالوژی سرچینو د منلو وړ کارونه تعریف کړئ، د کمپیوتر، شبکې، انټرنیټ او سافټویرونو تر څنګ ګڼ شمیر نورې برخې باید مشخص شي، تر څو دا سرچینې د پوهنتون د لید لوري او ماموریت په پام کې نیولو سره د علمي، تحقیقي، اداري او نورو مجاز اهدافو لپاره وکارول شي.

2.5. د کارونکي مسؤلیتونه: د معلوماتي تکنالوژی سرچینې مناسب او مسؤلانه کارونې په لړ کې د کارونکو مسؤلیتونه په ګوته کوي، د کاپي حق قوانینو ته درناوی، د حساسو معلوماتو ساتنه، او د هغو فعالیتونو څخه ډډه کول چې کیدای شي شبکې یا نورو کارووونکو ته د کارونو د خنډ او ځنډ او یا ګډوډۍ سبب وګرځي.

3.5. د کارونې حسابونه (یوزرونه) او پټ رمزونه (پاسورډونه): د کارونې حسابونو او پاسورډونو جوړولو او اداره کولو لپاره لارښوونې مشخص کوي، کاروونکي هڅوي چې قوي پاسورډونه غوره کړي، په منظمه توګه د ټاکل شوو وختونو په نظر کې نیولو سره بدل کړي، او له نورو سره یې شریک نه کړي، د حساب فعالولو، غیر فعالولو لپاره پروسیجرونه باید واضح او تعریف شوي وي.

4.5. د معلوماتو محرمیت: د معلوماتو د محرمیت او امنیت فعالیتونو او کړنو ته باید وده ورکړي، لکه د ډیټا کوډ کول، منظم بیک اپ، او د محرمیت اړوندو مقرراتو ته غاړه ایښودل، د حساسو معلوماتو اداره کول او د معلوماتو سرغړونو یا امنیتي پیښو راپور ورکولو لپاره باید طرز العملونه او د رسیدګۍ میکانیزمونه مشخص شي.

5.5. د شبکې کارول: د شبکې کارولو لپاره مقررات باید رامینځته شي، په شمول د غیر مجاز لاسرسي محدودیتونه، هیک کول او د غیر مجاز وسیلو کارول، د (Bandwidth) محدودیتونه باید په ګوته شي، د شبکې ځارنه او د شبکې ناوړه ګټه اخیسته یا غیز مجاز لاسرسي مخنیوي لپاره اقدامات باید تعریف شي.

6.5. د سافټویر کارول: د پوهنتون ملکیت وسیلو کې د سافټویر نصب او کارولو لپاره لارښوونې باید مشخص شي، د جواز لرونکو سافټویرونو کارول، د سافټویر د غلا کولو مخنیوي، او د غیر مجاز یا احتمالي زیان رسونکي سافټویر نصبولو محدودیتونه په ګوته کړي.

7.5. بریښنالیک او اړیکې: د پوهنتون د بریښنالیک او مخابراتي سیستمونو مناسب کارولو لپاره باید لارښوونې چمتو کړي، مسلکي او په درناوي ولاړه اړیکه وهڅوي، او ځینې فعالیتونه لکه سپیم کول، فشینګ، یا هغه لینکونه چې باید ونه لیږل شي منع کول، همدارنګه د پوهنتون د رسمي بریښنالیکونو د بیک او مراقبت لپاره لارښوونې او سیستمونه باید تعریف کړي.

8.5. ریموټ لاسرسي او VPN: د پوهنتون سرچینو ته د لیرې لاسرسي لپاره لارښوونې، پشمول د مجازي شخصي شبکو (VPNs) کارول، د پوهنتون د چاپیریال څخه بهر ځایونو څخه د پوهنتون سیستمونو ته د لاسرسي لپاره امنیتي اړتیاوي او لارښوونې او د محرمو معلوماتو د خوندي ساتلو لپاره لارښوونې باید شاملې وي.

9.5. د کارکوونکو شخصي وسایل: د پوهنتون په شبکه کې د شخصي وسایلو کارولو لپاره باید پالیسي او لارښوونې تعریف شي، د شخصي وسیلو څخه د پوهنتون سرچینو ته د لاسرسي لپاره امنیتي اړتیاوي، د وسیلې ثبت کول او نورې اړینې لارښوونې او اصول واضح او مشخص شي.

10.5. اطاعت: د لوړو زده کړو وزارت، مخابراتو وزارت د تطبیق وړ قوانینو او مقرراتو او د پوهنتون د پالیسیو او طرز العملونو سره د موافقت په اهمیت باید ټینګار وشي، د نه اطاعت کولو پایلې په ګوته شي لکه د انضباطي عملونو یا د معلوماتي تکنالوژۍ د خدماتو او امتیازاتو د لاسه ورکول.

11.5. ښوونه او رزونه: د معلوماتي تکنالوژۍ د پالیسیو، امنیتي غوره کړنو او د معلوماتي تکنالوژۍ د سرچینو مسؤلانه کارونې په اړه د پوهاوي وده او روزنیزو برنامو چمتو کول، تر څو کارووونکي وهڅوي چې د راپورته کیدونکو احتمالي ګواښونو او تکنالوژیکي بدلونونو په اړه خبر شي.

12.5. تطبیق او څارنه: د معلوماتي تکنالوژۍ د سرچینو د څارنې، د پالیسۍ سرغړونو پلټنه، او د اړتیا په وخت کې د پایلو پلي کولو لپاره طرز العملونه باید تعریف شي، همدارنګه د معلوماتي تکنالوژۍ په برخه کې د ملاتړیو او همکارو کارمندانو رول او د پالیسۍ سرغړونو لپاره د راپور ورکولو هر ډول تګلارې (میکانیزمونه) په ګوته شي.

اوومه ماده: د معلوماتي تکنالوژۍ دندیز مکلفیتونه

7.1: د سیستمونو مدیریت: د پوهنتون د کمپیوټري شبکې، سرورونو، انټرنیټ، برښنایي سیستمونو (LMS, MIS, EMS...)نصب، تنظیم ، څارنه او کارووونکو لپاره د لاسرسي (Access) مدیریت.

7.2:هارډویر او سافټویر مدیریت: د کمپیوټرونو، پرنټرونو، سکینرونو او نورو وسایلو ارزونه، نصب، ترمیم او تازه کول **او** د قانوني سافټویرونو تنظیم، جوازونه، او د اړتیا پر بنسټ پراختیا

7.3:د ویب‌پاڼې او ټولنیزو شبکو همغږي: د پوهنتون رسمي ویب‌پاڼې تنظیم، او نشراتو سره په هماهنګۍ کې د پوهنتون د ټولو رسمي اکاونټونو امنیت ساتل.

7.4:د برښنایي زده‌کړو ملاتړ: د E-learning سیستمونو (Moodle, Google Classroom, Zoom...) تنظیم، ملاتړ او روزنه او د پوهنتون د بریښنایې زده کړو کمیټېو سره د استادانو او محصلینو لپاره تخنیکي اسانتیاوې برابرول

7.5:د امنیت او محرمیت تضمین: د پوهنتون معلوماتي سیستمونو لپاره د امنیت پالیسۍ ترتیب **او** د معلوماتو خوندي‌ساتنه، معیاري Backup، او لاسرسي کنټرول.

7.6:روزنه او مشوره: د مسلکي پرمختیا مرکز سره په همغږۍ د استادانو، کارکوونکو او محصلینو لپاره د IT روزنیز پروګرامونه تنظیمول او د نویو تکنالوژیو په برخه کې مشورې ورکول

7.8:د همکاریو پراختیا: د پوهنتون د رهبرۍ په اجازه د ملي او نړیوالو IT بنسټونو، شرکتونو او شبکو سره همکاري او د نوې تکنالوژۍ او تجهیزات راجلبول

7.9:د راپور ورکونې سیستم: د فعالیتونو، ستونزو، اړتیاوو او لاسته راوړنو راپور برابرول او اداري ته سپارل.

7.10:په ربعوار او کلنې ډول مالي او اداري چارو مرستیال او علمي شورى ته راپور ورکول.

7.11:په ټولو برخو کې د IT اړوند ستونزو د حل په موخه په وخت اقدام کول.

7.12:د پوهنتون له ټولوې ډیجټلي وسایلو څخه وخت په وخت څارنه او کتنه کول.

7.13:پوهنتون له ټولو اجرائیوي واحدونو په منظم ډول د Soft Data ترلاسه کول او پوهنتون ارشیف په عمومي هارډسک کې خوندي او محرم ساتل.

7.14:د پوهنتون له سرورخونې، کمپیوټر لېب، امنیتي کمرو، اداري کمپیوټرونو او ټولو تکنالوژیکي وسایلو څخه د فعالیت په موخه ډاټا ترلاسه کول.

7.15:د ډیټابیس چاري مخ ته وړلو ترڅنګ د ډیټابیس له استعمال سره د اداري کارکوونکو او استادانو بلدول او ټرېننګونه ورته برابرول.

7.16:نورې ټولې هغه دندې چې د پوهنتون د لوړو مراجعو لخوا ورته سپارل کیږي.

اتمه ماده: د ډیټا او معلوماتو آمنیت

د ډیټا او معلوماتو امنیت په پوهنتون کې د معلوماتي تکنالوژۍ د پالیسۍ یوه مهمه او اساسي برخه ده، پدې برخه کې د پوهنتون په داخل او د بهر څخه تهدید کیدونکو مواردو او امنیتي اندیښنو لپاره لارښوونې او کړنې تعریف شوي، چې د ډیټا او معلوماتي شتمنیو ساتنه، محرمیت، بشپړتیا، شتون او د هغې څخه دوامداره نظارت تضمینوي، د معلوماتي تکنالوژۍ دا برخه د معلوماتو طبقه بندي کولو، د معلوماتو اداره کولو، ذخیره کولو، لاسرسي کنترول، ستونزو او پیښو ته رسیدګي او غبرګون، راپور ورکولو، کوډ کولو او تصدیق کولو تر څنګ د فزیکي امنیت پورې اړونده فعالیتونو او اقداماتو اغیزمنتیا باندې تمرکز کوي.

1.8. د معلوماتو طبقه بندي: د معلوماتو طبقه بندي د معلوماتو د درجه بندي کولو پروسه ده چې د هغې د حساسیت، ارزښت او د پوهنتون د اړتیاوو پر بنسټ وي، د معلوماتو د ډلبندۍ یو قوي سکیم (Scheme) پوهنتون ته وړتیا ورکوي چې د معلوماتي تکنالوژۍ په برخه کې خپلو سرچینو ته د هغوي د طبقو پر بناء لومړیتوب ورکړي، او مناسب امنیتي تدابیر او کنترول ورته پلي کړي، پوهنتون د حساسیت او انتقاد پر اساس د معلوماتو طبقه بندي کولو اهمیت پیژني، معلومات ممکن په څو کچو طبقعه بندي شي لکه عامه، داخلي، محرم او خورا محرم ، دا طبقه بندي د محافظت او ساتنې لپاره د مناسبې کچې په پیژندلو کې مرسته کوي او ډاټا ترلاسه کوي چې معلومات د هغې د طبقه بندۍ پر اساس سم اداره کیږي، حفظ او زیرمه کیږي او اړونده برخو سره شریک کیږي.

2.8. د معلوماتو اداره کول او ذخیره کول: د پوهنتون د معلوماتو د خوندي کولو لپاره د ډیټا سم اداره کول او ذخیره کول اړین دي، پالیسي د معلوماتو د جوړولو، عملیه کولو، ذخیره کولو، لیږد او ضایع کولو په اړه لارښوونې وړاندې کوي، دا د ډیټا ذخیره

کولو لپاره د خوندي میتودونو او تصویب شویو ځایونو کارولو باندې ټینګار کوي، د حساسې ډیټا کود کول او د معلوماتو خوندي تصفیه کول، کله چې اړتیا ورته نه وي.

3.8. د لاسرسي کنترول: حساسو معلوماتو او سیستمونو ته د غیر مجاز اشخاصو د لاسرسي مخنیوي لپاره د لاسرسي کنترول خورا مهم دی، د دې فرعي برخې هدف د پوهنتون د معلوماتي تکنالوژۍ زیربنا کې د لاسرسي کنترول قوي میکانیزم رامینځته کول دي، پدې کې د کارونکي تصدیق، د واک ورکولو پروسیجرونه، د کارونکي حساب مدیریت، او د امتیازاتو لاسرسي مدیریت لارښوونې شاملې دي، باید ډاډ ترلاسه شي چې ډیټا او سیستمونو ته لاسرسی د مشروع اړتیاوو پر اساس ورکول کیږي او په منظم ډول د نظارت او بیا کتنې لاندې نیول کیږي، او په اړونده برخو کې د واکونو د زیاتوالي او کموالي په اساس پکې اجراات صورت نیسي.

4.8. پېښو او ستونزو ته ځواب او راپور ورکول: سایبریایي امنیت کولی شي د معلوماتي تکنالوژۍ په برخه کې د پوهنتون د اړونده څانګو فعالیتونه زیانمن او ګډوډ کړي، دا فرعي برخه د پېښې اغیزمن ځواب او د راپور ورکولو چوکاټ رامینځته کولو باندې تمرکز کوي، دا د پېښو د راپور ورکولو لپاره طرز العملونه په ګوته کوي، د پېښې غبرګون په جریان کې رول او مسؤلیتونه ټاکي، او د پراختیا روښانه بهیر رامینځته کوي، د یو ښه او تعریف شویو پېښو غبرګون پلان په درلودلو سره پوهنتون کولی شي د امنیتي پېښو اغیز کم کړي، په چټکۍ سره ګواښونه کم کړي او د اغیزمنو سیستمونو او معلوماتو په وخت کې سمدستي ترمیمات او بیا رغونه ترسره کړي.

5.8. کوډ کول او تصدیق کول: کوډ کول او تصدیق کول د معلوماتو د لیږد پر مهال د خوندي کولو لپاره حیاتي امنیتي اقدامات دي، ددې فرعي برخې موخه داده چې د پوهنتون په معلوماتي تکنالوژۍ اړونده برخو کې د کوډ کولو او تصدیق کولو معیارونه رامینځته کړي، پدې کې د کوډ کولو لپاره لارښوونې شاملې دي، د اړونده برخو د مدیریت کلیدي کړنې، خوندي تصدیق میتودونه او د څو فکتور تصدیق کارول شامل دي د قوي کوډ کولو او تصدیق کولو اقدامات پلي کولو سره پالیسي د حساسو معلوماتو محرمیت او خوندیتوب ته وده ورکوي.

6.8. فزیکي امنیت: فزیکي امنیتي تدابیر د پوهنتون د معلوماتي تکنالوژۍ د زیربنا او د پوهنتون په احاطه کې ساتل شوي اړونده حساسو معلومات لپاره مهم دي، دا برخه د فزیکي امنیت کنترول او نظارت لپاره لارښودونه رامینځته کولو باندې تمرکز کوي ، لکه سرور خونو ته د لاسرسي کنترول، امنیتي کمرو او د معلوماتو مرکزونو او نورو مهمو برخو کې د لاسرسي کنترول شامل دی، پدې کې د تجهیزاتو امنیت لپاره اقدامات شامل دي پالیسي باید ډاډ ترلاسه کړي چې فزیکي امنیت خطرونه په ګوته شوي تر څو د معلوماتي تکنالوژۍ شتمنیو ته د غیر مجاز لاسرسي، غلا یا زیان مخه ونیسي.

نهمه ماده: شبکه او زیربناء

تابش کې د شبکې او زیربناوو پالیسي د پوهنتون د شبکې سرچینو مدیریت، کارولو او امنیت لپاره لارښوونې او طرز العملونه رامینځته کوي، ددې برخې موخه د پوهنتون د اکاډمیک او اداري چاپیریال او فعالیتونو ملاتړ لپاره د باور وړ، خوندي او لوړ فعالیت لرونکې شبکې زیربنا چمتو کول دي د پالیسۍ دا برخه مختلف اړخونه پوښوي لکه د شبکې لاسرسی، د بیسیم شبکې کارول، د شبکې څارنه او امنیت، د تجهیزاتو او سافټویر معیارونه او د شبکې فعالیت او اصلاحي اقدامات تعریفوي.

1.9. شبکې ته لاسرسی: د شبکې د لاسرسي په برخه کې د پوهنتون شبکې سرچینو ته د لاسرسي لپاره مقررات او طرز العملونه په ګوته کوي دا تعریفوي چې څوک د شبکې لاسرسي لپاره وړ دي، په شمول د محصلینو، استادانو، اداري کارمندانو او د پوهنتون سره وصلیدونکو اشخاصو او میلمنو، پالیسي د کاروونکو انفرادي کړنو لپاره د سندونو په کارولو سره د هغوي تصدیق وکړي او په غیر مجاز لاسرسي محدودیتونه پلي کړي، دا ممکن د منلو وړ کارونې پالیسي هم مشخص کړي او همدارنګه هغه فعالیتونه باید په ګوته شي چې په شبکه کې مجاز یا منع شوي وي.

2.9. د بې سیم شبکې کارول: دبیسیم شبکې کارولو په برخه کې د پوهنتون په چاپیریال او خواو شاه برخو کې د بیسیم شبکې اداره کول شامل دي، د بیسیم شبکې سره د نښلولو او کارولو لپاره باید لارښوونې تعریف شي پشمول د شبکې ته د

لاسرسي، د امنیت ډاډمن کولو پروسیجرونه، د بیندې ویټ د محدودولو لپاره شرایط، تر څو د ټولو کارونکو لپاره د انټرنیت او شبکې غوره فعالیت څخه ډاډ یقیني شي.

3.9. د شبکې څارنه او امنیت: د شبکې نظارت او امنیت د پوهنتون د شبکې زیربنا د غیر مجاز لاسرسي، معلوماتو سرغړونو او نورو امنیتي ګواښونو څخه د ساتنې لپاره اقدامات رامینځته کوي، دا د امنیتي پیښو کشف او مخنیوي لپاره د شبکې څارنې وسیلو او تخنیکونه په ګوته کوي ، پدې کې ممکن د اور وژنې الات، د ننوتلو (داخلیدو) کشف سیستمونو او د بهرنیو ګواښونو په وړاندې د ساتنې نور امنیتي تدابیر شامل وي او همدارنګه د وسیلو او معلوماتو امنیت ساتلو کې د کارونکو مسؤلیتونو تعقیبول شامل وي.

4.9. د تجهیزاتو او سافټویرونو معیارونه: د تجهیزاتو او سافټویرونو په برخه کې د شبکې وسیلو نصب شوي ډولونه لکه روټرونه، سویچونه او د لاسرسي نقطې چې د پوهنتون شبکې سره وصل کیدای شي، پدې برخه کې ممکن په څو شکله کې کارول شویو وسیلو او سافټویرونو لپاره لږ تر لږه تخنیکي مشخصات او د مطابقت اړتیاوي په ګوته شي او د وسایلو او سافټویرونو په معیاري کولو سره د شبکې په زیربنا کې د نه مداخلې، اعتبار او امنیت ډاډ یقیني کړي.

5.9. د شبکې فعالیت: د شبکې فعالیت او اصلاح کول په پوهنتون کې د لوړو فعالیتونو او اغیزمنې شبکې زیربنا ساتلو باندې تمرکز کوي، په دې کې د ظرفیت پلان کولو، د شبکې ډیزاین ، بیندې ویت تخصیص لپاره ستراتیژي (تګلاري) او نور فعالیتونه شامل دي، پدې کې ممکن د شبکې منظمې ارزونې، د څارنې وسایل پکار اچول، او د اصلاح لپاره لازم او مناسب تخنیکونو څخه کار اخیستل شامل دي، تر څو د فعالیت خنډونه وپیژندل شي او سمدلاسه حل شي، او د باور وړ او ځواب ورکوونکي شبکې چاپیریال کارکوونکو ته چمتو او غوښتنې پوره شي.

لسمه ماده: بریښنالیک او اړیکې

د تابش پوهنتون په اداري او علمي چاپیریال کې د بریښنالیکونو او اړیکو برخه د ارتباطي چینلونو د مناسبې کارونې لپاره لارښوونې او توقعات رامینځته کوي، پدې کې د بریښنالیک استول او ترلاسه کولو، فوري یا عاجل پیغام رسولو، همکارۍ وسیلې، ټولنیزو رسنیو، د امنیت او محرمیت لوړول او اداري کارمندانو، استادانو او محصلینو تر منځ د اړیکو او همکارۍ اغیزمنه فضاء رامینځته کول دي، دا د پوهنتون لخوا د چمتو شوي بریښنالیک حسابونو د منلو وړ کارول په ګوته کوي او د رسمي اړیکو، اداري او علمي فعالیتونو لپاره د دوي په مطلوب هدف باندې ټینګار کوي د پوهنتون د بریښنالیک حسابونو په کارولو سره کارووونکي کولی شي ډاډ ترلاسه کړي چې د دوي اړیکه د اداري په چوکاټ کې خوندي پاتې کیږي.

1.10. د بریښنالیک حسابونو جوړول: د پوهنتون د معلوماتي تکنالوژۍ آمریت باید د اداري، علمي برخو کارکوونکو او همدارنګه د پوهنتون سره د نوو یوځای شوو استادانو او یا هم د ځانګړو موخو لپاره د بریښنالیک ادرسونو جوړولو لپاره د غوښتنلیک او د هغې د تائیدۍ سیستمونه ایجاد کړي، هره څانګه چې غواړي د پوهنتون رسمي بریښنالیک حساب ترلاسه کړي نو پدې برخه کې باید د تائیدۍ د پروسیجر څخه طی مراحل شي، او له هغې وروسته د معلوماتي تکنالوژۍ آمریت له لورې ورته د بریښنالیک حساب ترتیب او د کارونې په اړه ملومات ورکړي.

2.10. د بریښنالیک حسابونو کارول: د پوهنتون د بریښنالیک حسابونو کارونه د نومورو حسابونو هدف او ساحه په ګوته کوي ، دا مشخص کوي چې دا حسابونه د رسمي پوهنتوني داخل او بهرنیو اړیکو (معلوماتو غوښتلو او ورکولو) لپاره دي پدې برخه کې باید د معلوماتي تکنالوژۍ آمریت د رسمي بریښنالیک حسابونو د جوړولو او سپارلو ترڅنګ د هر کارمند څخه د بریښنالیک د کارونې عمومي اصولنامه لاسلیک او حفظ کړي تر څو د کاري دورې په جریان کې د انفرادي بریښنالیک حسابونو اداره کولو، لاسرسي او نورو برخو په اړه کارمندانو ته عامه پوهاوي صورت نیولی وي چې یاد انفرادي حسابونه د اداري لخوا د څارنې تابع دي تر څو د پوهنتون د اهدافو، پالیسیو او مقرراتو سره اطاعت یقیني کړي.

3.10. د بریښنالیک اداب او مسلکیت: دا برخه د بریښنالیک اداب او مسلکي کارونې لپاره لارښوونې رامینځته کوي، لکه ورکشاپونه، رونیزې ناستې چمتو کوي تر څو د روښانه او هر اړخیزو اړیکو اهمیت په اړه د پوهنتون کارکوونکو ته روزنه ورکړي، دا د درناوي او مهربانۍ ژبې په کارولو ټینګار کوي چې د مناسبو موضوعاتو، سلسله مراتبو، سلامونو، لاسلیکونو، عادي او عاجل موضوعاتو، د ایمیل د متن، د (CC) او (BCC) په اړه د لارښوونو او همدارنګه د بریښنالیکونو د ځانګړو ډولو لپاره د ټیمپلیټونو یا معیاري فارمیټونو کارول وهڅوي تر څو ثابت او مسلکي اداري چاپیریال یقیني کړي.

4.10. د بریښنالیک امنیت او محرمیت: د بریښنالیک امنیت او محرمیت ډاډ ترلاسه کولو لپاره د حساسو معلوماتو خوندي کولو میکانیزمونه باید په ګوته شي، لکه د کارووکو لپاره لارښوونې، ددوي د بریښنالیک حسابونو لپاره قوي او ځانګړي پاسورډونه، منظم او معیاري پټ نومونه، د تصدیق او تائید اړونده برخو فعالول، کارکوونکو ته د سایبر حملو او فیشینګ حملو او د هغې د سمدلاسه راپور ورکولو په اړه رزونې، د محرمو معلوماتو لیږدولو لپاره د خوندي بریښنالیک چینلونو کارول، د غیر معیاري ایمیلونو او یا ویبسایټونو نه تعقیبول (Subscriptions) او همدارنګه په بریښنالیک کې د هر ډول امنیتي پښنو راپور ورکولو په برخه کې لازم او شفاف طرز العملونه او تګلارې باید رامینځته او تعقیب شي.

5.10. د ټولنیزو رسنیو لارښوونې: د پالیسۍ دا برخه کارکوونکو ته د هغوي د شخصي او همدارنګه د پوهنتون د رسمي ټولنیزو صفحاتو د کارولو لپاره لارښوونې وړاندې کوي، تر څو د ټولنیزو رسنیو د ډولونو په تفکیک د خپل ځان او پوهنتون په مسؤلیت سره د استازیتوب کولو په اړه لارښوونې وړاندې کړي، پدې کې ممکن ورکشابونه، د پوهاوی کمپاینونه او د نورو لارو چارو څخه کارووکو ته د ټولنیزو رسنیو د مناسبې کارونې په اړه پوهاوی ورکړي تر څو کارمندان د نامناسبو یا غیر اخلاقي مینځپانګو له خپرولو څخه ډډه کول، د فکري ملکیت حقوقو ته درناوی او په انلاین زده کړو او پیغامونو کې د مثبتو پیغامونو په نشرولو باندې ټینګار کول دي، تر څو د ټولنیزو رسنیو پورې اړوند مسایلو یا پښنو ته د رسېدو لپاره طرز العملونه او تګلارې باید مشخص شي.

یولسمه ماده: سافټویرونه او اپلیکیشن

د تابش پوهنتون په اداري او علمي چاپیریال کې د سافټویر او اپلیکیشن پالیسي په ټوله اداره کې د یادو برخو لپاره د سافټویر او اپلیکیشن غوښتنه، نصب، کارول او مدیریت کول اداره کوي، دا د سافټویر د نصب د جواز ورکولو سره موافقت تضمینوي، د اغیزمن او خوندي سافټویر کارولو ته وده ورکوي د پوهنتون لخوا د سافټویرونو، او اپلیکیشنونو کارولو لپاره لارښوونې په ګوته کوي د خلاصې سرچینې (Open Source) سافټویرونو لارښوونې په ګوته کوي، او د کلاوډ کمپیوټري خدماتو کارولو لپاره تګلارې رامینځته کوي په ټوله کې د دې برخې موخه داده چې د پوهنتون په چاپیریال کې د سافټویرونو د نصب، اداره کولو، کنترول او تعقیب لپاره سیستمونه رامینځته او د هغوي د اغیزمنتیا کچه لوړه کړي او د اداري سرچینې په موثره توګه وکارول شي او معلومات خوندي وساتل شي.

1.11. د سافټویرونو استملاک (خریداري): د پالیسۍ دا برخه په پوهنتون کې د معلوماتي تکنالوژۍ په برخه کې د هر ډول سافټویرونو د استملاک (خریداری) د جواز ورکولو میکانیزمونه په ګوته کوي، دا د سافټویرونو په تدارکاتو کې دخیلې ځانګې، پروسې او اړخونه په ګوته کوي لکه ، د غوښتنلیک کتنه، معلومات ورکول، انتخابول، ارزونې او د هغې تصویبول، پدې کې ممکن اداري چارو آمریت او معلوماتي تکنالوژۍ آمریت او یا هم د دې پروسې د ارزولو لپاره ځانګړې کمیټه ایجاد شي، تر څو د سافټویر اړتیا ارزونه ترسره کړي، د جواز ورکولو ټرون د محتوا کتنه وکړي، اړونده برخو سره مجالس ترسره کړي.

2.11. د سافټویر نصب او تازه کول: د خوندي او تازه سافټویر کارولو ډاډ ترلاسه کولو لپاره پالیسي د سافټویر نصبولو او تازه کولو لپاره میکانیزمونه چمتو کوي دا چاره ممکن د سافټویر د مجاز کارکوونکي او یا هم د سافټویر د پلي کولو او تازه کولو مرکزي سیستم له لارې ترسره شي، پدې برخه کې باید د سافټویر د تازه کولو او نورو معلوماتو لپاره لارښوونې رامنځته او تعقیب شي،

پدې برخه کې ځینې میکانیزمونه لکه پیچ مدیریت (Patch Management Systems) سیستمونه یا اتوماتیک تازه کول د سافټویر امنیت او فعالیت تضمین کول او د ستونزو په برخه کې راپور ورکونه او رسیدګي.

3.11. د پوهنتون لخوا چمتو شوي اپلیکیشنونه: د پوهنتون لخوا چمتو شویو اپلیکیشنونو د کارولو میکانیزمونه په ګوته کوي ، د پوهنتون لخوا چمتو شوي او نصب شوي سافټویرونه او اپلیکیشنونه او د هغوی د کارونې اهداف مشخص کوي او ډاډ ترلاسه کوي چې دا د اداري د ماموریت او اهدافو سره سمون لري، پدې برخه کې ممکن یادو سافټویرونو ته د لاسرسي میکانیزمونه، د کارونکي مسؤلیتونه، د معلوماتو امنیت او محرمیت او د منلو وړ کارونې پالیسیو ته غاړه ایښودل په ګوته کړي همدارنګه د یادو سافټویرونو لپاره د معلوماتي تکنالوژۍ لخوا د رزونې اړونده برنامې او تګلاري تر څو د کارووونکو سره مرسته ترسره شي چې ذکر شوي سافټویرونه په موثره توګه وکاروي.

په ټوله کې د پوهنتون په علمي او اداري چاپیریال کې د سافټویر او هر ډول اپلیکیشن د استملاک، نصب، کارولو او مدیریت لپاره میکانیزمونه رامینځته کوي، د دې میکانیزمونو په پلي کولو سره پالیسي د جواز ورکولو ټرونونو سره موافقت تضمینوي، د سافټویر اغیزمن او خوندي کارونې ته وده ورکوي د پوهنتون لخوا چمتو شوو سافټویرونو او اپلیکیشنونو کارولو لپاره لارښوونې چمتو کوي ، د خلاصې سرچینې سافټویر او د کلاوډ کمپیوټري خدماتو کارولو لپاره تګلاري روښانه کوي، د پالیسۍ دا برخه د پوهنتون د فعالیتونو سره مرسته کوي تر څو د خدماتو کچه لوړه کړي او د اداري سرچینې او امکانات او معلومات خوندي وساتل شي.

دولسمه ماده: هارډویر او تجهیزات

په پوهنتون کې د هارډویر او وسایلو پالیسي د معلوماتي تکنالوژۍ برخې د اداري چوکاټ یوه اړینه او مهمه برخه ده دا په پوهنتون کې د هارډویر او وسایلو د تدارکاتو، مدیریت، امنیت، تخریب ، حفظ او مراقبت او راپور ورکولو لپاره لارښوونې او طرز العملونه وړاندې کوي ددې برخې هدف د ټکنالوژیکي سرچینو شتون، اعتبار او امنیت ډاډمن کول دي، په اوسني ډیجیتل دور کې هارډویر او وسایل د پوهنتون د اکاډمیکو او اداري دندو په ملاتړ کې مهم رول لوبوي، لکه ډیسکټاپ کمپیوترونه، لپټاپ کمپیوترونه، ګرځنده وسایل اود شبکې زیربنا، دا تیکنالوژیکي شتمنۍ د اغیزمنې اړیکې، همکاري، ځیرنې، عصري تدریس او نورو زده کړیزو فرصتونو لپاره خورا مهم او ګټور دي.

1.12. د کمپیوټرونو او وسایلو تدارکات: د کمپیوټر او وسایلو تدارکاتو پالیسي په پوهنتون کې د هارډویر او وسایلو د ترلاسه کولو لپاره لارښوونې او طرز العملونه په ګوته کوي دا د نویو کمپیوټرونو، لپټاپونو، سرورونو، د شبکې تجهیزاتو او نورو تیکنالوژیکي وسایلو د پیرودلو پروسه تعریفوي، پالیسي کیدای شي غوره پلورونکي، د بودیجې تخصیص او د تدارکاتو لپاره د تصویب پروسه مشخص کړي، دا ډاډ ورکوي چې پوهنتون د خپلو اکاډمیکو او اداري اړتیاو د ملاتړ لپاره د باور وړ، مناسب او ارزانه او با کیفیته هارډویر توکي ترلاسه کوي.

2.12. د شتمنیو مدیریت او موجودیت: د شتمنیو مدیریت او موجودیت د پوهنتون د هارډویر او وسایلو تعقیب او اداره کولو لپاره یو سیستماتیک چلند او تګلاري رامینځته کوي چې پدې کې د هرې شتمنۍ د توضیحاتو ثبتولو لپاره پروسیجرونه شامل دي لکه ماډل، سریال نمبر، موقیعت، تفصیل، ټاګ نمبر، دا پروسه ددې لپاره ترسره کیږي تر څو د شتمنیو د نظارت په صورت کې د وسایلو موجودیت په اسانۍ سره یقیني کړي، همدارنګه د تجهیزاتو د ژوند دوریي نظارت باید ترسره شي او د منظم حفظ او مراقبت پروسې وربانديې پلي شي تر څو د موثره ساتنې او ملاتړ ډاډ ترلاسه شي.

3.12. شخصي وسایل: د پالیسی دا برخه د پوهنتون په شبکه او سیستمونو کې د محصلینو، اداري کارمندانو او استادانو لخوا د شخصي وسایلو کارول اداره کوي، چې دا کار د اکاډمیکو اهدافو لپاره د شخصي وسایلو کارولو پورې اړوند لارښوونې، امنیتي تدابیر او مسؤلیتونه په ګوته کوي، پدې لړ کې باید شخصي وسایل چې د پوهنتون په شبکه کې کارول کیږي ثبت او راجستر شي تر څو د امنیت او محرمیت پروتوکولونو اطاعت (انټي ویروس سافټویر او کوډ کول) او د منلو وړ کارولو پالیسیو سره موافقت یقیني کوي.

4.12. د ګرځنده وسیلو امنیت: د ګرځنده وسیلو امنیت پالیسي د سمارټ فونونو، ټابلیټونو او نورو ګرځنده (Portable) وسیلو خوندي کولو باندې تمرکز کوي چې د پوهنتون د کارکوونکو لخوا کارول کیږي، دا د ګرځنده وسیلو سره تړلي خطرونه په ګوته کوي لکه د معلوماتو سرغړونې، غلا، غیر مجاز لاسرسی، او مالویئر انتانات، پالیسي ممکن پدې برخه کې د پټ نوم محافظت پلي کړي د وسیلې کوډ کول، ریمو پاکولو وړتیاوې او د ګرځنده وسیلو مدیریت سافټویر کارول (MDM).

دیارلسمه ماده: د کاروونکی تصدیق او پټ نوم (پاسورډ)

لکه څنګه چې تکنالوژي پرمختګ ته دوام ورکوي،نو پدې لړ کې د حساسو معلوماتو امنیت ډاډمن کول هم خورا مهم بلل کیږي، د ډیجیټل سیستمونو د ساتنې یو له خورا عامو میتودونو څخه د کارونکي تصدیق کول او د قوي پاسورډ پالیسي اختیارول دي، تحصیلي ادارات هغه بنسټونه دي چې د شخصي او محرمو معلوماتو پراخه اندازه اداره کوي دوي باید داسې اقداماتو او فعالیتونو ته لومړیتوب ورکړي تر څو د دوی سیستمونه خوندي کړي او د خپلو محصلینو، استادانو او کارمندانو د معلوماتو او سیستمونو محرمیت وساتي.د کارونکي تصدیق د یو فرد د هویت کولو پروسه ده چې سیستم یا سرچینو ته د لاسرسي هڅه کوي، دا د دروازې د ساتونکي په توګه کار کوي یعني مجاز کاروونکوته اجازه ورکوي، پوهنتون کولای شي خپلو ډیجیټل سرچینو او سیستمونو ته لاسرسي کنترول کړي او حساس معلومات د غیر مجاز لاسرسي یا ناوړه ګټې اخیستنې څخه خوندي کړي.

1.13. د کارن حساب جوړول او مدیریت: د کارن حساب **(User Account)** جوړول او مدیریت د نوي حسابونو رامینځته کولو او د پوهنتون په سیستمونو کې د موجوده حسابونو اداره کولو لپاره د طرز العملونو ایجاد شامل دي:

1.1.13. د حساب جوړولو پروسه: معلوماتي تکنالوژۍ آمریت باید د کارن حسابونو (User Account) جوړولو لپاره معیاري کړنلاره ولري لکه د راجستریشن پر مهال د اړینو معلوماتو راټولول لکه بشپړ نوم، د محصل یا کارمند هویت کارت او د اړیکو معلومات، د ورکړل شوو معلوماتو تصدیق باید ترسره شي تر څو د حساب جوړولو غوښتنې مشروعیت ډاډمن شي.

2.1.13. د رول پربنسټ لاسرسی: د کارونکي مختلف رولونه ممکن د پوهنتون په سیستمونو کې شتون ولري، لکه محصلین، استادان، کارمندان، مدیران، آمرین، هر رول باید د دوي د مسؤلیتونو او غوښتنو پر اساس د لاسرسي مناسب اجازتونه ولري، د کارن حسابونه باید مشخصو رولونو ته وټاکل شي او د لاسرسي اجازه باید د هغې مطابق ورکړل شي.

3.1.13. د کارن حساب چمتو کول: یو ځل چې یو حساب رامینځته شي دا باید د اړینو سرچینو او لاسرسي حقونو سره چمتو شي، پدې کې ممکن ځانګړي ډیټابیسونو، انلاین زده کړو پلیټ فارمونو، بریښنالیک حسابونو یا نورو اړوندو سیستمونو ته د لاسرسي ورکول شامل وي د لاسرسي چمتو کول باید د کارونکي رول او مسؤلیتونو پر اساس وي.

4.1.13. د حساب بیا کتنه او پلټنه: منظمې بیا کتنې او پلټنې باید ترسره شي تر څو ډاډ ترلاسه شي چې د کارونکي حسابونه لا هم معتبر فعال او اړین دي، د هغو اشخاصو سره مربوط حسابونه چې په پوهنتون کې یې دنده ترک (پریښودې) وي یا بدل شوي رولونه باید په چټکۍ سره غیرفعال یا لرې شي دا د کارونکي حساب ډیټابیس تازه اوخوندي ساتلو کې مرسته کوي.

2.13. د پاسورډ پیچلتیا او لارښوونې د قوي پاسورډونو ډاډ ترلاسه کولو او د غیر مجاز لاسرسي پر وړاندې محافظت لپاره معلوماتي تکنالوژی آمریت باید د پاسورډ پیچلتیا اړتیاوي او لارښوونې رامینځته کړي چې په لاندې ډول واضح کیږي:

1.2.13. د پاسورډ لږ تر لږه اړتیاوې: د پاسورډونو پالیسي باید لږ تر لږه د پاسورډ اوږدوالی مشخص کړي په ځانګړې توګه د ۸ څخه تر ۱۲ حروفو پورې دا باید د لویو او کوچنیو حروفو، شمیرو او ځانګړو حرفونو ترکیب ته هم اړتیا ولري.

2.2.13. د پاسورډ ختمول او بدلول: په منظم ډول د پاسورډ پای ته رسیدل باید پلي شي په ځانګړي ډول له هرو ٦٠ څخه تر ۹۰ ورځو پورې کارووونکي باید په وخت سره د دوي پاسورډونو بدلولو ته وهڅول شي دا د جوړ شویو پاسورډونو اوږدمهاله کارونې مخنیوي کې مرسته کوي.

3.2.13. د پټنوم تاریخ او بیا کارول: سیستم باید د پټنوم تاریخ وساتي ترڅو کارووونکي د پخوانیو پاسورډونو له بیا کارولو څخه مخنیوی وکړي، دا ډاډ ورکوي چې کارووونکي د هر پټنوم بدلون لپاره ځانګړي پاسورډونو رامینځته کوي.

4.2.13. د پاسورډ ځواک ارزونه: سیستم باید داسې میکانیزمونه ولري چې د جوړولو یا بدلون پرسوې پر مهال د پاسورډونو ځواک ارزونه وکړي، دا د عام نمونو، لغت ټکې یا په عام ډول کارول شوي پاسورډونو په چک کولو سره ترسره کیدای شي، کارووونکي باید وهڅول شي چې قوي پاسورډ غوره کړي که چیرې د دوي لومړنی انتخاب ضعیف وي.

3.13. د څو فکتورونو تصدیق کول: د څو فکتورونو تصدیق (MFA) د امنیت اضافه والي لپاره کارول کیږي، چې کارووونکو ته اړتیا لري تر څو د دوي حسابونو ته د لاسرسي لپاره د پیژندنې ډیری ډولونه چمتو کړي پدې برخه کې باید لاندې لارښوونې په نظر کې ونیول شي:

1.3.13. دوه فکتور تصدیق (2FA): کارونکي اړ دي چې د تصدیق کولو دوه مختلف ډوله فکترونه چمتو کړي په ځانګړي ډول یو څه چې دوي پوهیږي (پاسورډ) او یو څه چې دوي لري (لکه یو ځانګړي کوډ چې د دوي ګرځنده وسیلې ته لیږل شوی یا د تصدیق اپلیکیشن لخوا رامینځته شوی).

2.3.13.بایومیتریک تصدیق: معلوماتي تکنالوژی آمریت کولی شي بایومتریک فکترونو لکه د ګوتو نښې، د مخ پیژندنه یا د ایرس سکین (Iris Scans) د اضافي تصدیق میتود په توګه وکاروي بایومیتریک ډیټا د کارونکي حسابونو سره وتړل شي تر څو د معلوماتو امنیت او محرمیت خوندي وساتل شي.

3.3.13.د هارډویر ټوکن: فزیکي وسایل یا ټوکنونه لکه د (USB) کیلي یا سمارټ کارتونه، د تصدیق لپاره د یو وخت پاسورډونو یا کریپټو ګرافیک کیلي جوړولو لپاره کارول کیدی شي، دا ټوکنونه د امنیت اضافي اقداماتو لپاره اړین دي او ډیری وختونه د پاسورډونو سره په ترکیب کې کارول کیږي.

4.13. د پټنوم تنظیم او د بیرته راګرځولو تګلاره: په داسې شرایطو کې چې کارووونکي خپل پاسورډونه هیر کړي یا یې بیا تنظم کولو ته اړتیا ولري، معلوماتي تکنالوژی آمریت باید پدې برخه کې د بیا تنظیم یا بیارغونې مناسب پروسیجرونه ولري چې په لاندې ډول واضح کیږي:

1.4.13.پټنوم د بیا تنظیم کولو اختیارونه: کارووونکي باید د خپلو پاسورډونو بیا تنظیمولو لپاره ډیری اختیارونه ولري، لکه د امنیتي پوښتنو ځواب، د بریښنالیک له لارې د پټنوم بیا تنظیم کولو لینک ترلاسه کول.

2.4.13.پخپله د پاسورډ بیا تنظیم کول: د پټنوم یا پاسورډ د ریسیټ یا بیا تنظیم کول کارونکو ته اجازه ورکوي چې د معلوماتي تکنالوژۍ له مرستې پرته خپل رمزونه (پاسورډونه) پټ نومونه په خپلواکه توګه بیا تنظیم کړي.

3.4.13.د حساب بیرته راګرځولو پروسه: په هغه حالاتو کې چې کارووونکي نشي کولی خپل پاسورډونه د معیاري وسیلو له لارې بیا تنظیم کړي، د حساب بیرته راګرځولو قوي پروسه باید شتون ولري، پدې پروسه کې ممکن د هویت تصدیق کولو اضافي مرحلې شاملې وي لکه د شخصي پیژندنې معلومات چمتو کول یا د ټاکل شویو مسؤلو کارمندانو سره اړیکه نیول.

5.13. د حساب بندول او غیرفعالول: کله چې کارووونکي پوهنتون پریږدي یا ځینو نورو سرچینو او سیستمونو ته د لاسرسي اجازه نلري او یا هم ورنه اخیستل کیږي، د دوي حسابونه باید فسخ یا غیر فعال شي تر څو د غیر مجاز لاسرسي مخه ونیول شي.

1.5.13.د اکاونټ غیر فعالول: کله چې د پوهنتون سره د یو کارونکي ټرون پای ته ورسیږي، نو د دوي حساب باید سمدستي غیر فعال شي، پدې سره د پخوانیو کارووونکو د لاسرسي مخه نیول کیږي او د حساسو او محرمو معلوماتو امنیت تضمین کیږي.

2.5.13.د حساب ارشیف: په ځینو مواردو کې دا اړینه وي چې غیر فعال شوی حسابونه د یوې ټاکلې مودې لپاره د قانوني یا پلټنې موخو لپاره وساتل شي، دا حسابونه باید په خوندي ډول ارشیف شي او د فعال کارووونکي حسابونو څخه جلا شي، تر ټاکل شوي مودې وروسته غیر فعال شوي حسابونه باید د تل لپاره د سیستم څخه لیرې شي تر څو د احتمالي امنیتي خطرونه مخه ونیول شي.

څوارلسمه ماده: د ډیټا بیک اپ او ریکوري (بیا ترلاسه کول)

سافټ ډیټا او معلومات د پوهنتون لپاره ارزښتناکه شتمني ده، ځکه چې پدې کې حساس معلومات لکه د محصلینو سوابق، د ځیړنو مربوطه معلومات، مالي حسابونو معلومات او نور ګڼ اداري او علمي اسناد شامل وي، د دې معلوماتو د ساتنې او شتون د یقیني کولو لپاره پوهنتون باید د ډیټا بیک اپ او بیا ترلاسه کولو پروسیجرونه او سیستمونه ولري دا برخه په منظم ډول د ډیټا بیک اپ کولو او د ډیټا له لاسه ورکولو یا سیستم د ناکامۍ په صورت کې د بیرته ترلاسه کولو لپاره طرز العملونه او تګلارې په ګوته کوي، د ډیټا بیک اپ او ریکوری اصلي موخه د ډیټا ضایع کېدو اغیزې کمولو او د پوهنتون د فعالیتونو د دوام تضمین کول دي،چې په لاندې ډول واضح کیږي:

1.14. د بیک اپ فریکوني او ساحه: د ډیټا بیک اپ فریکونسي د ډیټا د انتقاد پر اساس تعریف کیږي مهم معلومات لکه د محصلینو سوابق، مالي معلومات، ویبسایټونه، بریښنالیکونه، ډیټابیسونه او داسې نور باید هره ورځ او یا هم په ټاکل شوي وخت بیک ته اړتیا ولري پداسې حال کې چې لږ مهم معلومات ممکن په میاشت، ربعه یا په مهالني ډول بیک اپ شي، د بیک اپ ساحو په شمول د ځانګړو فایلونو یا سیستمونو د بیک اپ لپاره باید واضح تعریفونه او مهالویشونه رامینځته او تعقیب شي.

1.1.14.د معلوماتو لیست او طبقه بندي: معلوماتي تکنالوژۍ آمریت باید د ډیټا جامع لیست ترتیب کړي تر څو مهم معلومات وپیژني او د هغې مطابق بیک اپ ته لومړیتوب ورکړي، ډیټا باید د هغې اهمیت او حساسیت پر اساس طبقه بندي شي.

2.1.14.د بیک اپ ډولونه: د بیک اپ بیلابیل ډولونه کارول کیدی شي لکه بشپړ بیک اپ، زیاتیدونکي بیک اپ یا توپیر لرونکي بیک اپ بشپړ بیک اپ ټول ډیټا سیستمونه په بر کې نیسي، زیاتیدونکي او توپیر لرونکي بیک اپ د ورستي بیک اپ راهیسې د بدلونونو په نیولو تمرکز کوي، د دې بیک اپ ډولونو ترکیب کولی شي د ذخیزه کلو ځای او بیک اپ وخت غوره کولو کې مرسته وکړي.

3.1.14.د بیک اپ مهالویش: د معلوماتو د اهمیت او د بدلونونو فریکونسي پر اساس د بیک اپ مهالویش باید رامینځته شي ، مهم معلومات ممکن هره ورځ یا د ټاکل شوي وخت په اساس بیک ته اړتیا ولري ، او یا هم د ځینو ستونزو او ګډوډیو په صورت کې په عاجل ډول بیک اپ ترسره شي.

4.1.14.د اتوماتیک بیک اپ وسیلې: د بیک اپ سافټویرونو یا وسیلو کارول کولی شي د بیک اپ پروسه منظمه طی کړي دا وسیلې کولی شي د بیک اپ دندې اتومات کړي، د بیک اپ پالیسۍ پلي کړي او د ننوتلو او راپور ورکولو فعالیت چمتو کړي، اتوماتیک بیک اپ انساني خطا خطر کموي او دوام تضمینوي.

2.14. د بیک اپ ذخیره او ځایونه: دبیک اپ لپاره د ذخیره کولو ځایونه او اختیارونه باید مشخص شي، د فکتورونو لکه د ډیټا حجم، د لاسرسي اړتیاوې، او امنیت په پام کې نیولو سره د بیک اپ ډیټا په فزیکي میډیا کې زیرمه کیدای شي لکه ډیسکونه یا د کلاوډ ذخیره کولو سیستمونه دا ذخیره د فزیکي زیانونو یا افتونو په وړاندې د ساتنې لپاره کارول کیږي.

1.2.14.د اف سایټ ذخیره کول: د بیک اپ ډیټا باید په خوندي اف سایټ (Offsite) ځای کې زیرمه شي، یا په Cloud سیستمونو کې ذخیره شي، د ذخیره کولو ساحې او اسانتیاوو ته باید مناسب فزیکي او منطقي امنیتي تدابیر چمتو شي، په شمول د لاسرسي کنترول، کوډ کول او د بې ځایه کېدو څخه مخنیوي کول.

2.2.14. ستونزو (ناورین) د بیا رغولو پلان جوړونه: پوهنتون باید د ناورین د بیا رغونې هر اړخیز پلان رامینځته کړي چې د ناورین په صورت کې د معلوماتو او خدماتو د بیرته ترلاسه کولو لپاره ګامونه او طرز العملونه په ګوته شوي وي پدې پلان کې باید رول او مسؤلیتونه، د اړیکو پروتوکولونه، د بیا رغونې لپاره د مهمو سیستمونو لومړیتوبونه شامل وي.

3.2.14. د ناورین د بیا رغونې منظمه ازموینه: د ناورین د بیا رغونې پلان باید په منظم ډول وازمایل شي تر څو د پلان اغیزمنتوب تائید شي، په ازمایښت کې د مختلف ناورین سناریو سمول او د بیا رغونې پروسیجرونو پلي کول شامل دي، دا په پلان کې د هر ډول ضعف په پیژندلو کې مرسته کوي او ډاډ تر لاسه کوي چې د بیا رغونې پروسه د اړونده پرسونل لخوا په ښه توګه مستند او د پوهې کچه لوړه ده.

3.14. د معلوماتو ساتل او ارشیف کول: د بیک اپ لپاره د ساتلو موده باید مشخصه وي او د معلوماتو ارشیف کولو لپاره لارښوونې رامینځته شوې وي، د ساتلو موده ممکن د قانوني اړتیاو، مقرراتو سره د موافقت او د معلوماتو کارولو نمونو پر بنسټ توپیر ولري، د ارشیف کولو کړنلاره باید ډاډ ترلاسه کړي چې معلومات په خوندي ډول د اوږدې مودې ساتنې لپاره زیرمه شوي او د اړتیا په صورت کې بیرته ترلاسه کیدی شي.

1.3.14. د ساتلو پالیسي: معلوماتي تکنالوژۍ آمریت باید د ساتلو پالیسي تعریف کړي،څو دا مشخص کړي چې څومره وخت مختلف ډوله ډیټا باید وساتل شي، دا پالیسي باید قانوني او تنظیمي اړتیاوې، د صنعت معیارونه او داخلي اړتیاوې په پام کې ونیسي، د ساتلو موده کیدای شي د معلوماتوپه ډول پورې اړه ولري.

2.3.14. د ارشیف کولو پروسیجرونه: ارشیف کول د ځانګو څخه عمومي ارشیف ته د معلوماتو لیږدول شامل دي، پدې کې د مهالویش او پروسیجر مطابق لازم اسناد، او یا هم د ځینو پروژیې کارونو اسناد لکه د محصلینو د فراغت وروسته د هغوي اسناد او یا هم د یو ځانګړي فعالیت د بشپړیدو وروسته د هغې اسناد ارشیف کول.

3.3.14. د ارشیف د معلوماتو شاخصونه ټاکل: د ارشیف سیستمونه، اسناد او معلومات باید د شاخص په اساس ګټګوري شي تر څو د ارشیف شویو معلوماتو اغیزمن لټون او ترلاسه کولو اسانتیا رامینځته کړي، مناسب لېستونه یې باید ترتیب او د هغې د

ګډو او کلونو په اساس ثبت شي، تر څو کارووونکو ته اسانتیا رامینځته شي چې مشخص معلومات په چټکی سره بیرته یې ترلاسه کړي.

4.3.14. د معلوماتو بشپړتیا او امنیت: د ارشیف سیستمونه باید د ساتلو دوره کې د معلوماتو بشپړتیا او امنیت وساتي، پدې کې د پلي کولو اقدامات شامل دي لکه معلومات کوډ کول، د لاسرسي کنترول او د معلوماتو د صحت او بشپړتیا کتنه ترسره کول تر څو ډاډ ترلاسه شي چې ارشیف شوي معلومات د غیر مجاز یا لاسوهنې پر وړاندې خوندي دي.

4.14. د بیک اپ ازموینه او اعتبار: د بیک اپ منظمې ازموینې او اعتبار د دوی بشپړتیا او اعتبار ډاډمن کولو لپاره خورا اړین دي پدې کې باید د بیک اپ ازموینې ترسره کولو او د معلوماتو د بېرته راګرځیدو تصدیق کولو شرایط شامل وي پدې کې د معلوماتو له لاسه ورکولو سناریوګانو او د احتمالي مسایلو پیژندلو او حل کولو لپاره د بیارغونې تمرینونه ترسره کول شامل وي.

1.4.14. د بیک اپ لاګ او راپور ورکول: د بیک اپ فعالیتونو تفصیلي لاګونو او راپورونو ساتل پشمول د بریالي بیک اپونه، ناکام بیک اپ، او کومې تیروتنې او ستونزې چې په دې پروسه کې رامینځته شوي وي دا لاګونه د نمونو په پیژندلو کې مرسته کوي چې د بیک اپ فعالیتونه تعقیب کړي او هغه ستونزې حل کړي چې د بیک اپ په پروسه کې رامینځته شوي وي.

2.4.14. منظمه بیاکتنه او پلټنه: د بیک اپ زیربنا، طرز العملونو او لاګونو دوره ایزه بیا کتنه او پلټنه ترسره کول، تر څو ډاډ ترلاسه شي چې د بیک اپ پالیسي سره مطابقت لري دا بیا کتنې د بیک اپ په پروسې کې د تشې یا ضعف برخې پیژندلو کې مرسته کوي او دوامداره پرمختګ ته وده ورکوي.

5.14. د پیښې ځواب او بیارغونې پروسیجرونه: پالیسي به د معلوماتو له لاسه ورکولو، سیستم ناکامۍ یا ناوړینونو په صورت کې د معلوماتو بیارغونې لپاره ګام په ګام طرز العملونه په ګوته کړي، پدې کې د مسؤل پرسونل پیژندنه، د ارتباطي چینلونو تعریف کول، د پیښو د غبرګون پلانونه او دا پلانونه باید په منظمه توګه نوي او تمرین شي تر څو د دوي اغیزمنتوب ډاډمن شي.

1.5.14. د کارووونکو زده کړه او پوهاوی: منظم رونیز پروګرامونه او د پوهاوي کمپاینونه ترسره کول تر څو د پوهنتون کارمندانو ته د معلوماتو د ساتنې غوره عملونو او تمرینونو په اړه روزنه ورکړي، پدې کې د ډیټا بیک اپ اهمیت، د خوندي ډیټا اداره کول او د امنیتي تدابیرو د تعقیب په اړه معلومات شامل وي.

2.5.14. د لاسرسي کنترول او تصدیق: د لاسرسي قوي کنترولونه او د تصدیق میکانیزمونه باید پلي شي تر څو ډاډ ترلاسه شي چې یوازې مجاز اشخاص کولی شي مهمو معلوماتو او ډیټا ته لاسرسی ولري او یا یې هم تغیر کړي پدې کې د قوي پاسورډونو کارول، د څو فکتورونو تصدیق پلي کول، او د رول پر اساس د لاسرسي کنترول شامل دي.

6.14. امنیت او د لاسرسي کنترول: د بیک اپ ډیټا لپاره امنیتي اقدامات باید په ګوته شي پشمول د کوډ کولو، لاسرسي کنترولونو، تصدیق کولو میکانیزمونو بیک اپ ډیټا باید د ذخیره کولو او لیږد پر مهال د غیر مجاز لاسرسي یا لاسوهنې څخه خوندي شي، بیک اپ ته لاسرسی باید یوازې مجاز (مسؤلو) کارمندانو پورې محدود وي.

7.14. د کارمندانو روزنه او پوهاوی: د پوهنتون کارمندانو ته د ډیټا بیک اپ او بیارغونې پروسیجرونو اهمیت په اړه د پوهاوي لپاره باید مناسب رونیز او د پوهاوی پروګرامونه ترسره شي، کارمندان او غړي باید د پالیسۍ په اغیزمنه توګه پلي کولو کې د دوي د رول او مسؤلیتونو سره اشنا وي، روزنه د معلوماتو محافظت او د معلوماتو د لاسه ورکولو احتمالي پیښو د راپور ورکولو لپاره غوره او اغیزمن تمرینونه باید ترسره شي.

پنځلسمه ماده: معلوماتي تکنالوژی خدماتو مدیریت

د معلوماتي تکنالوژی خدماتو مدیریت (ITSM) د پوهنتون په علمي او اداري برخو کې د معلوماتي تکنالوژی خدماتو اداره کولو اصول، لارښوونې او تګلارې په ګوته کوي، دا د پوهنتون چاپیریال ته د موثره او اغیزمن معلوماتي تکنالوژی ملاتړ وړاندې کولو لپاره چوکاټ رامینځته کوي، چې په لاندې ډول د اصلي او فرعي برخو او اړخونو لپاره پیژندنه او د هغې اړونده میکانیزمونه وړاندې کوي.

1.15. د پیښو او ستونزو مدیریت: دپیښو مدیریت د ستونزو رامینځته کېدو او د هغې د تعقیب او حل وروسته د نورمال معلوماتي خدماتو بیارغونه باندې تمرکز کوي ، پدې کې د پیښو پیژندلو، هغې ته د داخلیدو، طبقه بندي، لومړیتوب ورکولو، تحقیق او حل کولو طرز العملونه شامل دي، پدې کې د پیښو د زیاتوالي د مخنیوي او کاروونکو ته د اغیزمنو معلوماتو او خبراوي په اړه لارښوونې شاملې وي، همدارنګه د ستونزو مدیریت موخه د تکراري پیښو اصلي لاملونه پیژندل او په ګوته کول دي ، پدې کې د بشپړو تحقیقاتو ترسره کول، د اصلاحي کړنو پلي کول او د پیژندل شویو ستونزو او غلطیو او کاري حلونو مستند کول شامل دي.

2.15. د بدلون مدیریت: د بدلون مدیریت د پوهنتون د معلوماتي تکنالوژی زیربناء، سیستمونو او خدماتو کې په منظم او همغږي ډول د بدلونونو کنترول او پلي کولو باندې تمرکز کوي، د بدلون مدیریت پروسې کې د وړاندیز شویو بدلونونو اغېزو او خطرونو ارزونه، د مناسبو تصویبونو ترلاسه کول، د بدلون فعالیتونو پلان کول او اجراء کول، او د پلي کېدو وروسته د بیاکتنو ترسره کول شامل دي، د بدلون مدیریت پروسه کې باید دا یقیني شي چې بدلونونه په روانو فعالیتونو کې د لږ تر لږه خنډ سره پلي کیږي او په یاده پروسه کې احتمالي خطرونه پیژندل شوي، او د وړاندې پیشبیني شوي دي.

2.15. د خدماتو په برخه کې موافقتنامې: د خدماتو د کچې موافقتنامې د معلوماتي تکنالوژی او د کاروونکو ترمنځ د خدماتو موافقه شوې کچې تعریفوي، د پوهنتون په کاري چاپیریال او شرایطو کې د (SLAs) د معلوماتي تکنالوژی د خدماتو او تعقیب مختلف ډولونه او د ستونزو په لړ کې عاجل او عادي غبرګونونه او وختونه بیانوي، دا ټرونونه باید د معلوماتي تکنالوژی آمریت له لوري د هر نوي کارمند سره د معلوماتي سیستمونو د فعالیدو په صورت کې لاسلیک شي تر څو په چارو کې روښتیا، حساب ورکونه او د تعقیب واضح چینلونه رامینځته شي، په (SLAs) د شبکې، بریښنالیک، انلاین زده کړیز سیستمونه، ډیټابیسونه او د معلوماتي تکنالوژی نورې اړینې برخې شاملې دي.

3.15. د خدماتو کتلاګ او د غوښتنې مدیریت: په پوهنتون کې د معلوماتي تکنالوژی د سیستمونو او خدماتو او همدارنګه د غوښتنو او نورو ترتیبابو په لړ کې د خدماتو کتلاک یو لارښود دی چې د پوهنتون د معلوماتي تکنالوژی په اړه هر اړخیز معلومات چمتو او وړاندې کوي، پدې کې د نوو کارمندانو لپاره د معلوماتي تکنالوژی د سیستمونو عیارول، روزنې، د سافټویرونو نصبول، د حسابونو او اکاونټونو پرانیستل، د هارډویر په برخه کې د کاروونکو غوښتنې او نور اړین موضوعات شامل وي، دا د کاروونکو سره مرسته کوي چې خپلې اړتیاوي او هغې ته رسیدګي وپیژني او د تکمیلی پروسه اسانه او د کاروونکو رضایت ښه کړي.

په ټولیز ډول، د پوهنتون په ترتیب کې د (ITSM) کړنلارې ددې ډاډ ترلاسه کولو کې مرسته کوي چې د معلوماتي تکنالوژی خدمات په اغیزمنه توګه وړاندې کیږي، ستونزې او پیښې په چټکی سره حل کیږي، بدلونونه په موثره توګه اداره کیږي، د خدماتو کچه لوړه ځي او د اړتیا وړ موضوعاتو ته رسیدګي ترسره کیږي، او د کاروونکو غوښتنې په خپل وخت حل او فصل کیږي، د دې خدماتو په وړاندې کولو سره معلوماتي تکنالوژی آمریت خپلو خدماتو ته وده ورکوي او د یو ګټور، باوري او ډیجیتل چاپیریال په رامینځته کولو کې مؤثر ثابتیږي.

شپاړلسمه ماده: د ویب او انټرنیټ کارولو تګلارې

تابش پوهنتون کې د ویب او انټرنیټ کارولو پالیسي د ویب مینځپانګې کارولو، ویب پاڼې ته لاسرسي، ټولنیزو رسنیو، انټرنیټ فلټر کولو، ځارنې او د پوهنتون د انټرنیټي سرچینو شخصي کارولو په اړه لارښوونې او مقررات وړاندې کوي، د پالیسی موخه داده چې د انټرنیټ مسؤله او ګټوره کارونه ډاډمنه کړي د پوهنتون د شبکې او سیستمونو ساتنه وکړي او د ټولو کارووونکو لپاره خوندي او ټول شموله ډیجیتل کاري چاپیریال رامینځته او وده ورکړي.

1.16. د ویب منځپانګې مدیریت: د پوهنتون د ویب پاڼې د مینځپانګې مدیریت پالیسي د ویب مینځپانګې رامینځته کولو، تازه کولو او اداره کولو لپاره لارښوونې په ګوته کوي پدې کې د محتویاتو (اصلي او فرعي مینو ګانو اوبرخو) کیفیت، دقت، تړاو او د تطبیق وړ قوانینو او مقرراتو او د صنعت د معیارونو سره ورته والی شامل دی، پدې کې باید د پوهنتون د مختلفو څانګو رول او مسؤلیتونه شامل وي لکه د ویب پاڼې پراختیا، بیاکتنه، د معلوماتو تکمیلي، د معلوماتو تازه کول، د معلوماتو تغیر، د تصویب پروسه، زاړه معلومات حذف کول د اړتیا په اساس نوې برخې او معلومات اضافه کول شامل دي.

2.16. وب پاڼې ته د لاسرسي لارښوونې: ددې لپاره چې په پوهنتون کې ټول شمولیت ته وده او معلوماتو ته د مساوي لاسرسي اصول پلي شي معلوماتي تکنالوژۍ آمریت د ویب پاڼې د لاسرسي لارښوونې رامینځته او پلي کوي، پدې کې د ویب پاڼې منځپانګې د لاسرسي (WCAG) لارښوونې، د ویب سایټ سرورونو او سورس کودونو ته لاسرسي، د ویب سایټ په تعقیب د بریښنالیکونو سرورونو ته لاسرسي، د ویب سایټ (Dashboard) ته لاسرسي، د عکسونو، معلوماتو او نورو مواردو د بدلیدو برخو ته لاسرسي، د معلوماتو او خبرونو (News) تازه کولو په لړ کې لاسرسي شامل دی.

3.16. د ټولنیزو رسنیو کارولو لارښوونې: د ټولنیزو رسنیو کارولو لارښوونې د پوهنتون د اداري کارکوونکو، استادانو او محصلینو لخوا د ټولنیزو رسنیو پلیټ فورمونو کارول اداره کوي، پدې کې د منلو وړ چلندونه، اخلاقي معیارونه او د پوهنتون د استازیتوب لپاره لارښوونې بیانوي، د پوهنتون د رسمي ټولنیزو رسنیو حسابونو، د پوهنتون د اړونده فعالیتونو لپاره د شخصي حسابونو کارول، محرمیت، او د حساسو معلوماتو اداره کولو په اړه مقررات وضع کول دي، معلوماتي تکنالوژۍ آمریت پدې برخه کې باید د هر نوي کارمند سره د معلوماتي تکنالوژۍ د خدماتو ژمنلیک په لاسلیک کولو سره د اړونده مواردو څخه په تفصیلي ډول یادونه وکړي تر څو پدې برخه کې یاد آمریت ته د کارمندانو د سایبر ځورل، بدنامول او د فکري ملکیت د حقوقو ساتنه په صحیح او معیاري شکل ترسره کړي.

4.16. د انټرنیټ فلټر کول او څارنه: دانټرنیټ فلټر کولو او څارنې پالیسي هغه تګلارې په ګوته کوي چې د پوهنتون لخوا تصویب او وضع شوي څو د انټرنیټ سرچینو مناسبې کارونې ډاډ ترلاسه شي، په دې کې د ویب پاڼو فلټر کولو ټکنالوژۍ پلي کول وي تر څو ځینو ویب پاڼو ته لاسرسی محدود کړي، چې نامناسب یا د اکاډمیکو فعالیتونو پورې تړاو ونلري، پدې کې د انټرنیټ نظارت او څارنه هم شامله ده تر څو د غیر مجاز یا غیر اخلاقي ویب سایټونو د (Hotspot) کارول کشف او مخنیوي وکړي، همدارنګه د ډاونلوډ او اپلوډ سرعت څارنه او د کارونکو لپاره د انټرنیټ حد ټاکل او د هغې تعقیب او همدارنګه د کارووونکو لخوا د غټ سایزونو ډاونلوډ او اپلوډ څارنه او هغوي ته په رسمي بڼه د خبراوي تګلارې شاملې دي.

5.16. د انټرنیټ سرچینو شخصي کارونه: د پوهنتون د انټرنیټ سرچینو شخصي کارولو پالیسي د شخصي اهدافو لپاره د پوهنتون انټرنیټ سرچینو لکه د شبکې بینډ ویت او کمپیوټري تجهیزاتو کارول په ګوته کوي، پدې کې د نظارت او څارنې په صورت کې کارووونکو ته د شخصي کارونې اجازي ورکړل شوې کچه مشخص کړي ، د مسؤلانه کارونې لپاره لارښوونې، او همدارنګه د شبکې او نورو مسایلو په لړ کې د وضع شویو محدویدتونو تعقیب شامل دی، کارووونکو سره باید د لمړنیو لیدنو،

کتنو او روزنې په صورت کې د پوهنتون د انټرنیټ د شخصي کارونې یا د اجازې پرته کارونې په صورت کې احتمالي انضباطي پریکړې هم شریکې شي.

6.16. د تطبیق میکانیزمونه: د ویب او انټرنیټ کارولو لپاره د پوهنتون مختلف میکانیزمونه پلي کول چې په لاندې ډول ورځخه یادونه کیږي:

1.6.16. د پالیسی عامه پوهاوی: پالیسي باید ټولو اداري کارکوونکو، استادانو او محصلینو ته د مختلفو چینلونو او پروسو لکه د پوهنتون ویب پاڼه، د کارمندانو لارښود کتابونه، د لارښوونې برنامې، روزنیز او تمرینې سټیشنونه، او همدارنګه نویو کارمندانو ته د انفرادي او ګروپې ترینګونو له لارې واضح او روښانه شي.

2.6.16. لاسرسي کنترول: معلوماتي تکنالوژی آمریت کولی شي د تصدیق کولو میکانیزمونه پلي کړي لکه د کاروونکو نومونه، او پاسورډونه، د انټرنیټ سرچینو ته د لاسرسي تنظیم کولو او د انفرادي کاروونکو لپاره حساب ورکونې او تضمین میکانیزمونو پلي کول.

3.6.16. د شبکې د څارنې وسیلې: معلوماتي تکنالوژی آمریت باید د شبکې د څارنې وسیلې په کار واچوي تر څو د انټرنیټ کارولو تعقیب ترسره کړي، سرغړونې کشف کړي او احتمالي امنیتي ګواښونه وپیژني، دا وسیلې کولی شي د انټرنیټ ترافیک (Internet Traffic) بینډویت کارول او په انټرنیټي او معلوماتي تکنالوژی کې د کاروونکو د فعالیتونو تعقیب ترسره کړي.

4.6.16. د راپور ورکولو میکانیزمونه: د پالیسی سرغړونو یا د ویب او انټرنیټ کارولو پورې اړوند مشکوک فعالیتونو راپور ورکولو لپاره طرز العملونه رامینځته کول دي.

5.6.16. اطاعت او تطبیق: پوهنتون باید د معلوماتي تکنالوژی د کارونې او اصولو د تعقیب یوه با صلاحیته ځانګړې کمیټه یا مسؤلین وټاکي تر څو د پالیسی سره سم د څارنې او ارزونې او پلي کولو مسؤلیت ولري، پدې کې ممکن دوره ایزې پلټنې ترسره شي، د راپور شویو پېښو څېړنه او د پالیسی څخه د سرغړونو لپاره د مناسبو انضباطي اقداماتو پلي کول شامل وي، کمیټه یا مسؤل شخص باید د معلوماتي تکنالوژی په اصولو پوه مسلکي او تخنیکي شخص وي.

د ویب او انټرنیټ کارولو میکانیزمونه باید په منظمه توګه تجدید او بیا کتنه یې ترسره او تازه شي تر څو د مختلفو نویو ټکنالوژیو او سیستمونو او رجحاناتو او د پوهنتون د ویب او انټرنیټ کارونې پورې اړوند اصولو او مقرراتو د اړتیاوو سره سمون ولري، او همدارنګه د معلوماتي تکنالوژی آمریت باید د پورته میکانیزمونو او تعقیبي سیستمونو لپاره مختلف پروسیجر فورمونه، موافقه لیکونه او د عامه پوهاوي بروشرې ډیزاین او د پوهنتون د علمي او اداري برخو کاروونکو سره شریک کړي.

اولسمه ماده: د رسمي کمپیوترونو او بریښنایي وسایلو د کارونې تګلارې

په پوهنتون کې ډیسکټاپ او لپټاپ کمپیوترونه د علمي، اداري، څېړنیزو فعالیتونو او دندو لپاره خریداري او نصب شوي ، کمپیوترونه د استادانو، کارمندانو لپاره لازم توکي دي چې محصلینو ته اداري او تدریسي سهولتونه برابروي او وړاندې کوي، همدارنګه محصلین هم د پوهنتون له کمپیوتري شتمنیو څخه د خپلو زده کړو، کورنیو دندو او نورو عملي کارونو لپاره استفاده کوي، چې پدې برخه کې لاندې میکانیزمونه او تګلارې په پوهنتون کې د هر ډول رسمي لپټاپ او ډیسکټاپ کمپیوترونو د اداره کولو لپاره وړاندې کیږي.

د علمي او اداري برخو ټول کارمندان به اجازه ورکوي تر څو کمپیوترونه یې د معلوماتي تکنالوژی د مسؤلو کارمندانو له لورې په ځینو امنیتي او عاجلو مواردو کې اداره شي، تر څو ډاډ ترلاسه کړي چې د دوي سیستمونه (Up to date) دې او که نه؟ او د شتمنیو سم مدیریت یې ترسره کیږي او که نه؟

که چیرې ومومل شي چې د کوم کارمند په کمپیوتر کې غیر معیاري او بې جوازه نرم افزار (سافټویر) اچول شوي وي، نو د معلوماتی تکنالوژی مسؤل کارمندان به اړونده کارمند ته پرته لدې چې خبر ورکړي ممکن د لرې واټن، اتوماتیک او یا هم په فزیکي ډول غیر فعال او له منځه یوسي، ځکه یاد سافټویرونه د اعتبار وړ ندي او کیدای شي د پوهنتون مهمو معلوماتو ته ضرر ورسوي.

په کمپیوترونو کی د اړتیا وړ ټول سافتویرونه باید غوره او بې خطره وي، د پوهنتون کارکوونکي د ټولو هغو سافټویرونو قانونیت لپاره شخصي مسؤلیت لري، چې د معلوماتي تکنالوژی آمریت لخوا ندي نصب (انسټال) شوي.

1.17. هارډویر چمتو کول: د پوهنتون معلوماتي تکنالوژی آمریت باید لپټاپ او ډیسکټاپ کمپیوترونو او د دوي پرزه جاتو د شهرت لرونکو عرضه کوونکو څخه وپلوري تر څو د کمپیوتري زیربناوو سره کیفیت او د معیارونو سره مطابقت یقیني کړي، د هارډویر په برخه کې باید د کاروونکو د نوعیت په اساس اړونده تجهیزات غوره شي لکه محصلین، استادان او اداري کارمندان.

2.17. سافټویرونه او عملیاتي سیستمونه: ادارات اکثراً یو معیاري عملیاتي سیستم لکه (Windows, MacOS, or Linux) د خپلوفعالیتونو د مخته وړلو او دوام لپاره کاروي، پدې سیستمونو کې د فعالیتونو د کنترول او چارو ترسراوي په خاطر مختلف سافټویرونه او اپلیکیشنونه نصبوي، یاد سافټویرونه باید د معلوماتي تکنالوژی په هماهنګی نصب او د کار لاندې راشي، او همدارنګه د سافټویرونو (نرم افزار) د اپډیټ (تازه) ساتلو لپاره باید په ټاکل شویو دورو کې د آمریت د مسؤلینو سره معلومات شریک شي.

3.17. د کارونکي حساب مدیریت: معلوماتي تکنالوژی آمریت باید د امنیت او لاسرسي کنترول لپاره د کارونکي حساب مدیریت سیستمونه پلي او تعقیب کړي، پدې کې باید د معلوماتي تکنالوژی اړونده مسؤلین د کارکوونکو او محصلینو د رسمي هر ډول اکاونټونو د کارونې او د اړونده برخو د معلوماتو د تازه ساتلو راپورونه چمتو او د ځان سره وساتي او هغه حسابونه چې د ډیر وخت لپاره نه کارېږي باید تعقیب او یا غیر فعال شي.

4.17. د ویروس ضد او امنیت سافټویرونه: د مالویر، ویروسونو او نورو امنیت او محرمیت پورې مربوط ګواښونو په لړ کې د لپټاپ او ډیسکټاپ کارونې لپاره د امنیتي او ویروس ضد سافټویرونو په وسیله ساتنه ترسره شي، د سافټویرونو د فعالیتونو په وسیله د احتمالي ګواښونو کشف او له منځه وړلو کې مرسته کوي حساس معلومات خوندي کوي او د پوهنتون کمپیوتري چاپیریال په بشپړتیا او دوام کې مرسته کوي.

5.17. د کمپیوترونو، پرنټرونو او نټرنیټي وسایلو عمومي تګلارې: تابش پوهنتون د ټکنالوژیکي وسایلو څخه د سمې او اغېزمنې استفادې او د غیر ضروري او شخصي استعمال د مخنیوي په موخه د معلوماتي ټکنالوژی د وسایلو د استفادې لپاره عمومي تګلارې او لارښوونې وړاندې کوي، چې په لاندې ډول په څو فرعي برخو کې واضح کیږي.

1.5.17. ډیسکټاپ کمپیوترونه: هغه کارکوونکي چې د پوهنتون رسمي ډیسکټاپ کمپیوترونه کاروي مکلف دي چې د کمپیوتر کارولو پر مهال لاندې موارد په پام کې ونیسي:

1. د کمپیوټر پاکوالي او ساتنې ته ځانګړې پاملرنه وکړي.

2. لږ تر لږه دري میاشتې وروسته کارمند باید معلوماتي ټکنالوژی امریت ته د کمپیوټر د پاکولو لپاره مراجعه وکړي.
3. هغه ځانګې چې (UPS) کاروي کله چې کار پیل کوئ، ډاډ ترلاسه کړئ چې (UPS) فعال او کمپیوټر ورسره وصل دی.
4. د خپل کمپیوټر پاسورډ بل چا ته ورنکړي، که کمپیوټر د بل چا له خوا خلاص شي مسؤلیت یې د اړونده کارکوونکي په غاړه دی.
5. د کمپیوټر د مسؤل پرته په کمپیوټر کې د Flash Drive کارولو مخه ونیول شي.
6. په کمپیوټر کې د Anti-Virus په اړه ډاډ ترلاسه کول چې فعال دی او که نه،کچیرې غیر فعال وي نو سمدستي د معلوماتي ټکنالوژی امریت سره اړیکه ونیول شي.
7. د Flash Drive د کارولو په صورت کې یې لومړی په خپل کمپیوټر کې د موجود Anti-Virus په واسطه Scan کړئ، که ستاسو د کمپیوټر Anti-Virus نشي کولی د Flash Drive څخه ویروس له منځه یوسي، نو Flash Drive مه خلاصوئ او د ستونزې د حل لپاره معلوماتي ټکنالوژی امریت سره اړیکه ونیسئ.
8. تابش پوهنتون اړوند کمپیوټر هارډ ډیسک کې د شخصي عکسونو، ویډیویي فایلونو او شخصي فلمونو د ذخیره کولو مخه ونیول شي،که د پوهنتون په کمپیوټرونو کې شخصي عکسونه یا فلمونه وموندل شي، حذف کېږي او کارمند د شکایت حق نه لري.
9. پوهنتون اړوند فایلونه او اسناد په ځانګړو فولډرونو کې په ځانګړو نومونو سره په جلا Drives کې پریږدئ، د Format کولو او یا هم (Windows Installation) په صورت کې به ستاسو Data محفوظه وي او تاسو به وکولی شئ ژر تر ژره اړینه Data ترلاسه کړئ.
10. هیڅ کارکوونکی حق نه لري چې خپل کمپیوټر په خپلسري ډول نورو ته د لاسرسي لپاره پریږدي.
11. په یو وخت کې د څو انټرنیټي صفحو خلاصول ممکن په شبکې کې تخنیکي ستونزې رامینځته کړي د کنټرول په صورت کې به ستاسو انټرنیټي اړیکه منحل شي او د تکرار په صورت کې به ستاسو کمپیوټر قید شي.
12. لاوډسپیکر چې په کمپیوټر کې د شخصي موخو لپاره نصب شوی په رسمي وخت یې کې کارول منع دي.
13. د رسمیاتو پر مهال د انځورونو، فلمونو او موسیقۍ کتل او اوربدل په کلکه منع دي.
14. د پوهنتون په کمپیوټرونو کې د غیر ضروري سافټویر نصبول لکه د کمپیوټر لوبې او نور غیر ضروري پروګرامونه په کلک ډول منع دي.
15. هیڅ کارکوونکی حق نه لري چې خپل کمپیوټر په خپلسري ډول Format کړي او یا Installation پکې وکړي.

2.5.17. لپټاپ کمپیوټرونه: لپټاپ کمپیوټرونه د عصري دفتري چاپیریال او ننې عصر یوه لازمه برخه ګرځیدلې، د لپټاپ کمپیوټرونو په کارولو سره کارکوونکو ته په فعالیتونو کې اسانتیا رامینځته کوي تر څو خپل پلانونه په صحیح شکل تطبیق او د خپلو چارو څخه په واضح او منظم شکل راپور او حساب ورکړي، دا چې په اداراتو کې د هر ډول تعاملاتو لپاره تګلارې وجود لري نو په لاندې ډول د پوهنتون د کارمندانو لپاره څو لارښوونې وړاندې کیږي چې لپټاپ کمپیوټرونه کاروي:

1. د لپټاپ کمپیوټر بیټرۍ تر هغه مه پریږدئ تر څو چې ډیره ضعیفه شي، یعنې تر هغه چې کمپیوټر د بیټرۍ د چارج د نشتوالي له امله بند شي، همدا راز کله چې د لپټاپ چارج پوره شو له چارج څخه یې اوباسئ.
2. کله چې مو کمپیوټر بند کړ، په چارجر بریښنا قطع کړئ.
3. د لپټاپ کمپیوټر په نا مناسبو سطحو (کوچ، سپنج ، توشک او یا په داسې ځای کې چې داخل ته یې د هوا د ورتللو مخه ونیسي) له ایښودلو ډډه وکړئ.
4. د کم چارج او بریښنا د نشتوالي په وخت کې، سمدستي خپل فایلونه خوندي ځای ته انتقال کړئ او کمپیوټر بند کړئ.
5. کمپیوټرونه مو د باور وړ او خوندي انټرنیټي شبکو یا وایفای سره وصل کړئ.

6. کوشش وکړئ چې په اداره کې او تاسې پورې مربوطه هغه سافټویرونه او پروګرامونه چې زیات کاریدونکي وي او یا هم ستاسې ورته په ځینو ځانګړو وختونو کې اړتیا پیدا کیږي د معلوماتي تکنالوژی په هماهنګۍ یې انسټال او نصب کړئ.
7. په لپټاپونو کې د هر ډول ستونزو په صورت کې په سیستم کې نور تنظیمات مه ترسره کوئ، او په سمدستي توګه د معلوماتي تکنالوژی آمریت مسؤلینوته خبر ورکړئ.

3.5.17. پرنټر ، فوټوکاپي ماشین او سکینر: پرنټر په دفترونو کې د ډیجیټل اسنادو فزیکي کاپي تولیدولو لپاره کارول کیږي او فوټو کاپیر یو ماشین دی چې د چاپ شوی او یا په لاس لیکل شویو اسنادو د کاپي کولو لپاره کارول کیږي دا په دفترونو کې ددې لپاره کارول کیږي چې اسناد په موثره او ګړندۍ توګه چاپ کړل شي او همدارنګه سکینر هغه وسیله ده چې د فزیکي اسنادو، عکسونو یا نورو لیدونو په ډیجیټل بڼه بدلولو لپاره کارول کیږي د پورته دریو برخو د کارونې لپاره عمومي اصول او لارښوونې په لاندې ډول واضح کیږي:

1. په پرنټرونو، فوټوکاپي ماشینونو او سکینرونو باندې د رسمیاتو په پای کې بریښنا قطع کړئ او کله چې ذکر شوي تجهیزات چالان کړئ، انتظار وکړئ څو په بشپړ ډول د استفادې لپاره چمتو شي.
2. په پرینټر او کاپي ماشین کې د غیر معیاري او ماتو شویو کاغذونو د کارولو څخه باید ډډه وشي.
3. په هغه صورت کې چې په پرنټر او فوټوکاپي ماشین کې د کاغذ اندازه محدوده وي، باید په خپلسري ډول د خلاصیدو مخه ونیول شي.
4. معلوماتي ټکنالوژی امریت کارکونکي له شتون پرته په پرنټر، فوټوکاپي ماشین او سکینر کې د لاس وهلو څخه باید ډډه وشي.
5. هڅه وکړئ په دفتر کې د پرنټر، فوټوکاپي او سکینر د ځای پر ځای کولو ځای ته پام وکړئ، چې له فزیکي پلوه زیانمن نه شي او د دفتر ټولو همکارانو ته په اسانۍ د لاسرسي وړ وي.

4.5.17. ډیجیټل تلفیون: ډیجیټل تلیفون چې د انټرکام تلیفون په نوم هم پیژندل کیږي، د ارتباط وسیله ده چې معلولا د پوهنتون په احاطه یعني داخلي دفترونو کې د اړونده برخو د ښه هماهنګۍ او چارو د چټکوالي په موخه د کارکوونکو ترمینځ د غږیز ارتباط لپاره کارول کیږي، د یادو وسیلو د کارونې لپاره په لاندې ډول ځینې لارښوونې وړاندې کیږي:

1. د رسمي اړیکو لپاره په دفترونو کې ډیجیټل ټیلیفونونه نصب شوي، د غیر ضروري او شخصي تلیفونونو څخه باید ډډه وشي.
2. د ټلیفون لاین مصروف ساتلو څخه ډډه وکړئ.
3. کله چې له بل لوري سره خبرې کوئ، له بې ضرورته خبرو ډډه وکړئ او تواضع په پام کې ونیسئ.
4. هڅه وکړئ چې په دفتر کې د ټیلیفون کولو لپاره (داخلي) ټیلیفونونه وکاروئ.
5. په دفترونو کې ډیجیټل ټیلیفونونه د معلوماتي ټکنالوژی امریت د مسؤلینو له خوا کنټرولیږي د ستونزې د پېښیدو په صورت نوموړي امریت سره په اړیکه کې شئ.

5.5.17. عمومي لارښوونې: په پوهنتون کې د معلوماتي تکنالوژي آمریت چې د علمي او اداري برخو لپاره د سیستمونو او سهولتونو پراخه لړۍ لري باید په پوهنتون کې ټول اداري، علمي او خدماتي کارکوونکي او ښکیلي برخې لاندې عمومي اصول او لارښوونې په نظر کې ونیسي:

1. د شخصي چارو لپاره د ټکنالوژیکي وسایلو کارول د ناوړه ګټه اخیستنې څخه ګنډل کیږي.
2. معلوماتي ټکنالوژی امریت کارکوونکي د تخنیکي اسانتیاوو د برابرولو په موخه ګمارل شوي، نو د تخنیکي وسایلو د کارولو د کنټرول په برخه کې عمومي او بشپړ واک لري.
3. د تخنیکي وسایلو کاروونکي مکلف دي چې د خپلو دفترونو د تخنیکي وسایلو د کنټرول پر مهال د معلوماتي ټکنالوژی امریت کارکوونکو سره همکاري وکړي او د دفترونو د ټکنالوژیکي وسایلو لکه (کمپیوټر، پرنټر، فوټوکاپي ماشین او نور) د کنټرول پر مهال مشکل رامنځته نه کړي.
4. معلوماتي ټکنالوژی امریت کارکوونکي مکلف دي چې د ټکنالوژیکي وسایلو څخه د استفادې په برخه کې خپل راپور مالي او اداري چارو معاونیت ته وسپاري.
5. کارکوونکو ته شته کمپیوټرونه د پوهنتون د بودیجې له پیسو څخه ورکول کېږي، د هر کارکوونکي ایماني او وجداني دنده ده، چې د پوهنتون په ګټه یې ساتنې او سمې استفادې ته ځانګړې پاملرنه وکړي.
6. له کارکوونکو څخه په درنښت غوښتنه کیږي چې د ټکنالوژیکي وسایلو څخه د ناوړه استفادې مخنیوي په برخه کې د معلوماتي ټکنالوژی امریت سره بشپړه همکاري وکړي.

اتلسمه ماده: د کارکوونکو انفرادي اکاونټونه او مسؤلیتونه

په پوهنتون کې د علمي او اداري برخو کارمندان شخصي حسابونه لري او د پوهنتون د استازو په حیث د هغې د کارونې ځینې خاص مسؤلیتونه لري تر څو د پوهنتون د پالیسیو او پرسیجرونو لخوا اداره شي، د کارمندانو د شخصي اکاونټونو څخه د ترسره شوو هر ډول فعالیتونو او معلوماتو پر وړاندې هر کارمند شخصي مسؤلیت لري، او همدارنګه ټول احتیاطي تدابیر لکه د پټ نوم (پاسورډ) امنیت او د فایلونو محافظت، د غیر مسؤلو اشخاصو یا ادارو لخوا د دوی حسابونو او فایلونو ته د لاسرسي څخه مخنیوی، د غیر مسؤلو اشخاصو سره د پوهنتون د کمپیوترونو او شخصی کمپیوترونو او د ډیټابیس د اکاونټونو او همدارنګه د انټرنیټ د یوزرونو د پاسورډونو شریکول یا لاسرسي ورکول په کلکه توګه منع دي، هغه کارکوونکي چې خپل پټ نوم (پاسورډ) دریمې ډلې ته ښکاره کوي،په بشپړ ډول د هغو پایلو مسؤل دي چې د معلوماتو او اسنادو د افشاء کېدو باعث کیږي.

نولسمه ماده: انټرنیټي سیستمونو ته لاسرسی

تحصیلي بنسټونو کې انټرنیټي سیستمونو ته لاسرسی د ارتباطاتو او سرچینو چمتو کولو او وړاندې کولو ته اشاره کوي چې د علمي او اداري برخې کارمندان او محصلین د اداري، علمي او زده کړیزو موخو لپاره انټرنیټ کاروي، چې پدې برخه کې اداره د تدریس، څیړنې، زده کړې او اداري دندو د ملاتړ په موخه د انټرنیټي خدمتونه او زیربناء چمتو کوي، د پوهنتون د انترنیت په برخه کې هیڅ کارکوونکی حق نلري چې د پوهنتون معلوماتي سیستم ته د مسؤلو اشخاصو پرته د لاسرسي یا کوم بل سهولت اسانتیا برابره کړي، د انترنیت هیڅ کاروونکی حق نلري چې شخصي سویچونه، راوټرونه، د لاسرسي الې یا (DHCP) وسیلې د انترنیت د مرکزي شبکې سره وصل او ونښلوي، پرته لدې چې د اړونده وسایلو د مسؤل شخص او یا هم د معلوماتی تکنالوژی آمریت په تفاهم باید صورت ونیسي.

1.19. د انټرنیټي خدماتو څخه د ګټه اخیستنې شرایط: د یوې تحصیلي اداري په توګه چې خپلو استادانو، اداري او علمي کارمندانو، محصلینو ته د انټرنیټ خدمات او لاسرسی چمتو کوي نو په دې برخه کې د انټرنیټي خدماتو سم او مسؤلانه کارونې ډاډ هم باید ترلاسه کړي او ددې لپاره باید واضح او ښکاره شرایط او لارښوونې موجودي وي، دا شرایط او لارښوونې د خوندي او ګټور انلاین او ډیجیټل اداري او علمي چاپیریال په رامینځته کولو، د پوهنتون د شبکې بشپړتیا ساتلو او د انټرنیټ کارولو په اړه د قانوني او پوهنتوني مقرراتو مطابقت ډاډمنوي، پوهنتون د انترنیت څخه ګټه اخیستنه باید د پوهنتون د معلوماتی تکنالوژی آمریت لخوا د ټاکل شوو اصولو په رڼا کې ترسره شي، ځکه د پوهنتون د انترنیتي سیستم له لارې د پوهنتون نورو

ټولو الکترونیکي سرچینو ته لاسرسی پیدا کیږي، چې اړونده برخې او د هغوي معلومات د خطر سره مخ کوي، د پوهنتون د داخلي اصولو له مخې د انترنیت څخه د غلطې استفادې او سرغړونکو سره د اداري لخوا قانوني چلند ترسره کیږي، او د مجازاتو په پایله کې د شفاهي توصیې، لیکلې توصیې، لیکلي اخطار ، د دندې ځنډ او یا هم ګوښه کیدل شامل دي، چې یادې پریکړې به د پوهنتون د با صلاحیته او ټاکل شوو کمیټو لخوا ترسره کیږي.

شلمه ماده: د معلوماتي او انټرنیټي سیستمونو کارولو ممانعتونه

پوهنتون د معلوماتو او انټرنیټي سیستمونو کارولو په اړه ځانګړي مقررات او ممانعتونه لري تر څو ددې سرچینو مسؤله او قانوني کارونه ډاډمنه کړي دا بندیزونه د پوهنتون د شبکې د بشپړتیا ساتلو، د حساسو معلوماتو د ساتنې، او د قانوني مقرراتو سره مطابقت لپاره ځای پر ځای شوي دي، دا پوهنتون د ټولوغړو لپاره خورا مهم دي چې د خوندي او مناسب ډیجیتل چاپیریال رامینځته کولو لپاره ددې ممانعتونو څخه خبر وي او تعقیب یې کړي،

1.20. غیر مجاز لاسرسی: د پوهنتون د معلوماتو او انټرنیټ سیتسمونو حسابونو، ډیټا او نورو سیستمونو ته د غیر قانوني لاسرسي هر ډول هڅه په کله منع ده، لکه هیک کول، کریک کول، یا د امنیتي لارښوونو نه مراعتول او تېریدل شامل دي، پدې برخه کې د هر ډول ستونزو او د هغې د رفع او تعقیب مسؤلیت په پیل کې د معلوماتي تکنالوژی آمریت مسؤلو کارمندانو او په دوهم قدم کې د اړونده برخو د کارمندانو دی.

2.20. د معلوماتو امنیت: د پوهنتون د معلوماتو او انټرنیټي سیستمونو کارووونکي باید د معلوماتو محرمیت، او امنیت اصولو ته درناوی وکړي د شخصي، اکاډمیک یا مالي معلوماتو په ګډون د هر ډول حساسو معلوماتو غیر مجاز افشا کول ، بدلون او یا له منځه وړل په کلکه منع دي، پدې برخه کې د هر ډول لیدل شویو او کشف شویو ستونزو او یا راپورونو په اساس به د پوهنتون با صلاحیته مراجع تصمیم نیسي.

3.20. د فکري ملکیت سرغړونه: د معلوماتي تکنالوژی او انټرنیټي برخې کارووونکي باید په هر هغه فعالیتونو کې له ښکیلتیا څخه ډډه وکړي چې د فکري ملکیت حقونه نقض کوي، پدې کې د کاپي حق لرونکي موادو غیر مجاز ویش، بیا انکشاف یا تولید، یا شریکول شامل دي لکه سافټویر، ملټي میډیا ، فایلونه یا اکاډمیک، اداري زده کړیز او څېړنیز مواد.

4.20. ناوړه سافټویرونه او ویروسونه: په قصدي توګه د پوهنتون په معلوماتو او انټرنیټي سیستمونو کې د ناوړه سافټویرونو، ویروسونو یا کوم بل زیان رسونکي کوډ معرفي کول، خپرول یا نصبول په کله منع دي، کارونکي باید د فایلونو ډاونلوډکولو یا شریکولو په وخت کې احتیاط وکړي تر څو د مالویر د خطر او سیستم ته د ضرر رسونکو ویروسونو د انتقال څخه مخنیوي وکړي.

5.20. غیر قانوني کړنې: د پوهنتون د معلوماتو او انټرنیټ سیستمونو له لارې په هر ډول غیر قانوني فعالیتونو کې ښکیلتیا په کلکه منع ده ، لکه درغلی، غیز مجاز مالي تعاملات، ځوروني، تبعیض یا کوم غیر قانوني عمل چې د محلي، ملي یا نړیوالو او د صنعت د قوانینو منع تعریف شوي وي او په ټکر کې وي.

6.20. د شبکې ځنډ: د پوهنتون کارووونکي باید په داسې فعالیتونو کې ښکیل نه وي چې د پوهنتون د معلومات او انټرنیټ سیستم نورمال عملیات ګډوډ یا زیانمن کړي، پدې کې هغه فعالیتونه شامل دي چې د شبکې ډیزي سرچینې مصرفوي، د عادي او ټاکل شویو طرز العملونو څخه انکار کوي یا د شبکې ارتباط او فعالیت کې ګډوډي رامینځته کوي او مداخله کوي په کلکه منع دي او د واقع کیدو په صورت کې یې معلوماتي تکنالوژی آمریت د نظارت او څارنې لمرنی مسؤلیت لري او په اړه به یې با صلاحیته مراجع پریکړه کوي.

7.20. ناوره یا نامناسبه کارونه: د پوهنتون کاروونکي د معلوماتو او انټرنیټ له لارې د سپکاوي، فحش، یا نا مناسبو ویب پاڼو ته د لاسرسي، جوړولو یا خپرولو څخه په کلکه منع دي، پدې کې د تبعیض، ځورونکي، بدنامونکي یا بل ډول کړنې چې د پوهنتون د ارزښتونو او پالیسیو سره په ټکر کې واقع کیږي په کلک ډول منع دي.

8.20. د معلوماتي او انټرنیټي سیستمونو عمومي ممانعتونه: د پوهنتون د تخنیکي برخې کاروونکي باید انترنیت او معلوماتي سیستمونه په هیڅ صورت په غیر مسؤلانه، ضایع کوونکي او داسې ډول ونه کاروي چې په پوهنتون یا انترنیت کې په نورو کاروونکو، او یا هم نورو فعالیتونو او تجهیزاتو منفي اغیز وکړي، چې په لاندې ډول په عمومي ډول ورځخه یادونه کیږي چې په پوهنتون کې د ټولو ښکیلو برخو لپاره لارښوونې ټاکي او د یادو فعالیتونو څخه یې په کلک ډول منع کړی:

1. د فرد یا اشخاصو ځورونه، ګواښول، بدنامول او یا ډارول.
2. د یو غیر ټولنیز یا کرکه لرونکي عمل او یا موادو خپراوی، کوم چې د یو فرد یا یوې ډلې پر وړاندې د نژاد، مذهب، اصل، عمر، جنسیت، ازدواجي وضیعت، جنسي تعصب، جنیټیک جوړښت او معلولیت پر اساس د تبعیض او ځورونې لامل وګرځي.
3. د داسې معلوماتو خپرول چې سرغړونکی، تاوتریخوالی رامنځته کوونکی او فحشا خپرونکی وي.
4. د جعلي پیغامونو لېږل او د جعلي منځپانګو (اکاونټونو) رامنځته کول.
5. د پوهنتون د انترنیتي سیستم د پټو نومونو او رمزونو (پاسورډونو) خپرول او د غیر مسؤلو اشخاصو سره یې شریکول.
6. د پوهنتون هغه معلوماتو او سرچینو ته د لاسرسي ممانعت مراعت کول چې د پوهنتون لخوا ورته په لاسرسي پاپندي لګیدلې وي.
7. د پوهنتون د انترنیتي سیستم څخه د بلې اداري سیستم ته د لاسرسي پوښښ ورکول.
8. د هر ډول وسیلو په ذریعه تابش پوهنتون د معلوماتي سیستم یا شبکې د کومې برخې امنیتي میکانیزم ته لاسرسی، د معلوماتو ښکاره کول، خنډ پیدا کول او یا هم هیک کول.
9. د پوهنتون د معلوماتو بدلول، خرابول او یا له منځه وړل.
10. انترنیتي سیستم ته د وایروس او یا نورو مضرو پروګرامونو داخلول.
11. غیر قانوني، غولونکي او یا هم جعلي فعالیت ترسره کول.
12. د کاپي حق لرونکو د اجازې پرته د کاپي حق لرونکو معلوماتو ترلاسه کول او استعمالول.

پویشتمه ماده: د معلوماتي تکنالوژی په برخه کې د پوهنتون حقوق او مکلفیتونه

د کارمندانو پر وړاندې د معلوماتي تکنالوژی په برخه کې د پوهنتون عمومي حقوق او مکلفیتونه د پوهنتون په چاپیریال کې د تکنالوژی مسؤلیت او اخلاقي کارونې لپاره یو چوکاټ رامینځته کول دي، دا حقوق او مکلفیتونه هغه برخې، امتیازات او مسؤلیتونه په ګوته کوي چې کارمندان یې د معلوماتي تکنالوژی سرچینو په اړه لري. د ټیکنالوژی کارولو پورې اړوند مسؤلیتونو او امتیازاتو په ګوته کولو سره، د پوهنتون موخه د معلوماتو محرمیت ساتل، د فکري ملکیت ساتنه، او د ډیجیټل علمي او اداري کاري چاپیریال رامینځته کول او وده ورکول دي، تابش پوهنتون د معلوماتي تکنالوژی آمریت او د دغه سیستم د ټولو کاروونکو معلوماتو ته د غیر مسؤلو اشخاصو د لاسرسي او د یادو معلوماتو او سیستمونو څخه د ناسمې ګټې اخیستنې څخه باید مخنیوی وشي، د پوهنتون د معلوماتی تکنالوژی آمریت دا حق له ځان سره ساتي چې د خبرتیا او یا هم له خبرتیا پرته د عاجلې ستونزې په صورت کې د انترنیت کاروونکو د معلوماتو څارنه، ثبت او یا د کوم کاروونکی حساب (اکاونټ) محدود او یا هم بند کړي، همدارنګه د پوهنتون اداره حق لري چې وخت پر وخت یاد سیستمونه وپلټي او ددې معلوماتي سیستمونو ساتنې او خوندیتوب لپاره نور اړین اقدامات ترسره کړی، د معلوماتي تکنالوژی په برخه کې د پوهنتون د حقوقو ځینې کلیدي برخې په لاندې ډول ذکر کیږي:

1.21. د استخدام قراردادونه او ځانګړي تړونونه: کله چې کارکوونکي په پوهنتون کې تقرر حاصلوي، دوي عموما د کارمندۍ قرارداد یا تړون لاسلیک کوي چې د دوی د کار شرایط په ګوته کوي په شمول د معلوماتي تکنالوژۍ کارولو او دندیزو مسؤلیتونو پورې اړونده برخې، دا قراردادونه به د معلوماتي تکنالوژۍ سرچینې دمعلوماتو ساتنه، فکري ملکیت، او د منلو وړ کارولو په اړه اصول او لارښوونې ولري د یادو لارښوونو په تعقیب او ترسراوي کارمند مکلف دی او د سرغړونې په صورت کې به ورسره اصولي او قانوني اجراات ترسره کیږي.

2.21. د معلوماتي تکنالوژۍ روښانه لارښوونې او تګلارې: پوهنتون باید د معلوماتي تکنالوژۍ جامع پالیسي او لارښوونې رامینځته کړي، چې د کارمندانو حقوق او مسؤلیتونه پکې په روښانه توګه تعریف شوي وي دا تګلارې باید د منلو وړ کارولو، د معلوماتو محرمیت، فکري ملکیت، د معلوماتو امنیت، او سیستمونو ته د لاسرسي په برخه کې ساحې او تګلارې مشخص کړي، پالیسي باید کارمندانو ته د انلاین پورټلونو، کتلاګونو، لنډو او واضح لارښودونو، بینرونو او لاسي کتابونو (Handbooks) له لارې د لاسرسي وړ وي.

3.21. د کارمندانو تقرر په صورت کې روزنه: کله چې کارمندانو د پوهنتون د علمي او اداري برخې سره یوځای کیږي او تقرر حاصلوي، دوي باید د معلوماتي تکنالوژۍ آمریت د پالیسیو او لارښوونو په اړه لازمه او ساحې ته په کتو سره روزنه ترلاسه کړي، دا روزنه باید دوی ته د دوي د حقوقو او مکلفیتونو او همدارنګه د پالیسۍ د سرغړونو احتمالي پایلو په اړه روزنه ورکړي، دا روزنه د مختلفو ګروپي او انفرادي ورکشاپونو او سیمینارونو له لارې ترسره کیدای شي.

4.21. رضایت او اعتراف: پوهنتون باید د معلوماتي تکنالوژۍ آمریت د پالیسۍ او نورو اړینو لارښوونو د پوهېدو او منلو په اړه د کارمندانو څخه په لیکلي ډول څرګند او واضح رضایت او اعتراف ترلاسه کړي، دا د لاسلیک شوو فورمونو، لیکونواو ایمیلونو د تبادلې څخه ترلاسه کیدای شي.

5.21. د لاسرسي کنترول او د کارونکي حسابونه: پوهنتون باید د لاسرسي کنترول او د کارونکي حساب مدیریت سیستمونه پلي کړي تر څو ډاډ ترلاسه کړي چې کارمندان د دوي د رول او دندیزو مسؤلیتونو پر اساس د معلوماتي تکنالوژۍ سرچینو ته مناسب لاسرسی لري، پدې کې اړونده کارمندانو ته د رسمي تائید شوو فورمونو او ټاکل شوو پروسیجرونو پر اساس واک او مسؤلیت ورکول کیدای شي.

6.21. محرمیت او د ډیټا محافظت تدابیر: پوهنتون باید د کارمندانو معلوماتو خوندي کولو لپاره مناسب محرمیت او د ډیټا محافظت اقدامات او سیستمونو عیار او پلي کړي، پدې کې کوډ کول، د څو لارو د تصدیق پروسې، د لاسرسي کنترول، منظم ډیټا بیک اپ سیستمونه او د خوندي ذخیره کولو عملي تمرینونه شامل دي، د پوهنتون معلوماتي سیستمونه ، پیغامونه، بریښنالیکونه، فایلونه، ضمیمې، ګرافونه، او انترنیت چې پدې سیستم کې او یا ددې سیستمونو له لارې رامنځته کیږي د پوهنتون ملکیت دی، او د پوهنتون د کوم کارمند، دایمي استاد، قراردادي کارمند، استاد، محصل او یا هم کوم شخص شخصي ملکیت نه شمیرل کیږي، ټول بریښنایي مخابرات، فایلونه، اکاونټونه چې د تابش پوهنتون د شبکې له لارې لیږدول شوي، زیرمه شوي او کتل شوي وي د پوهنتون د معلوماتی تکنالوژۍ آمریت له لورې په دوامداره توګه څارل کیږي او د ځانګړو میتودونو او وسیلو په واسطه خوندي کیږي، تر څو محرمیت یې په ښه شکل وساتل شي.

7.21. د پېښو راپور ورکول او اداره کول: پوهنتون باید دکارمندانو لپاره یو میکانیزم رامینځته کړي تر څو د معلوماتي تکنالوژۍ پېښو، امنیتي ستونزو او سرغړونو، یا د پالیسۍ د سرغړونو راپور ورکړي، دا د یو معلوم او واضح پروسجر په وسیله ترسره کیږي یا

د معلوماتي تکنالوژۍ آمریت سره د مستقیمې اړیکې له لارې ترسره کیدای شي پوهنتون باید روښانه کړنلاره ولري تر څو راپور شوې پیښې په سمدستي توګه وڅیړي او حل یې کړي، او کارووونکي باید اړونده ستونزې په سمدستي توګه راپور کړي.

8.21. ادبي غلا او د علمي تیروتنو کشف کول: د پوهنتون اداره حق لري چې د ادبي غلا او علمي تیروتنو د مخنیوي په پار د معلوماتي تکنالوژۍ پرمټ د استادانو او محصلینو لخوا د ورسپارل شویو علمي څېړنو، مقالو، مونوګرافونو او نورو علمي او تحقیقاتي اثرونو او موادو څیړنه او پلټنه وکړي، او ددې برخې لپاره د (Plagiarism) او نور پرمختللي سافټویرونه او سیستمونه رامینځته کړي، او د هغې له مخې د اړونده څانګو سره په ګډ تفاهم ستونزه کشف او د حل لپاره یې رسیدګي وکړي.

9.21. دوره یي پلټنې او بیا کتنې: پوهنتون باید د معلوماتي تکنالوژۍ سیستمونو، پالیسیو او کړنلارو په اړه دوره ایزې پلټنې او بیا کتنې ترسره کړي، تر څو د پوهنتون د اهدافو، ارزښتونو، لیدلوري او ماموریت سره موافقت یقیني کړي، او د پرمختګ لپاره ساحې وپیژني، دا پلټنې کولی شي د هر ډول تشو یا زیانونو په پیژندلو کې مرسته وکړي او پوهنتون ته اجازه ورکوي چې په اړونده برخو کې اصلاحې کړنې او ګامونه واخلي.

10.21. انضباطي کړنې او تطبیقات: د پالیسۍ د سرغړونو په صورت کې پوهنتون باید د انضباطي کړنو د پیژندلو، معلوماتو راټولولو، تحلیل کولو، پربکړه کولو لپاره روښانه لارې او مراجع وټاکي، پدې کې ممکن د شفاهي توصیې، لیکلي توصیې، لېکلې اخطاریې، د دندې ځنډ، تعلیق او یا هم د دندې ګوښه کول شامل وي، هره پربکړه په اړونده برخه کې د سرغړونې د شدت او خفت پورې اړه لري او په اړه به یې پریکړه باصلاحیته کمیټه یا مرجع کوي.

دوه ویشتمه ماده: د معلوماتي تکنالوژۍ څارنه او ساتنه

په تحصیلي بنسټونو کې د معلوماتي تکنالوژۍ آمریت (IT) لپاره څارنه او ارزونه (M&E) یوه مهمه پروسه ده چې له پوهنتون سره مرسته کوي تر څو د معلوماتي تکنالوژۍ سیستمونو، زیربنا، او خدماتو اغیزمنتوب ، موثریت او په اړونده برخو کې د اغیز څارنه او ارزونه وکړي، په دې کې د فعالیت اندازه کولو لپاره په سیستماتیک ډول د معلوماتو راټولول، تحلیل او راپور ورکول شامل دي، تر څو د پرمختګ لپاره ساحې وپیژندل شي، د معلوماتي تکنالوژۍ سیستمونو او فعالیتونو ته وده ورکړل شي او د پوهنتون د لیدلوري، ماموریت او ستراتیژیکو اصلي او فرعي اهدافو ملاتړ لپاره باخبره او منتظمې پریکړې ترسره شي.

1.22. د هارډویر څارنه او ساتنه: د هارډویر د برخو لکه سرورونو، شبکې تجهیزاتو، انټرنیټي سیستمونو، کمپیوټر سیستمونو، سوچونو او لینونو د منظمې څارنې او ساتنې لپاره مهالویش ترتیبول، چې په مهالویش کې به د پاکوالي، پوره والي، ځانګړې تمرینونو ترسره کول او د دې څارنو منظم او عیني راپورونه د اړونده شواهدو او معیارونو په کتنه ترتیبول شامل وي، دا به د معلوماتي تکنالوژۍ د تجهیزاتو د عمر په زیاتوالي کې مرسته وکړي.

2.22. د سافټویر څارنه او ساتنه: په منظم ډول د سافټویرونو او اپلیکیشنونو او همدارنګه عملیاتي سیستمونو، ډیټابیسونو، ویبسایټونو د معلوماتو او ورځنونو تازه کول، د زیان رسونکو برخو په نښه کول، په اړونده برخو کې فعالیتونو ته وده ورکول او د راځرګندیدونکو ګوابنونو پر وړاندې د خوندیتوب اقدامات شامل دي، دا هم باید د څارنې او ساتنې په پلان کې شامل وي او د سافټویرونو د کتنې او تازه کولو اړونده معیارونه او وختونه باید پکې په مشخص ډول ذکر شوي وي، دا به د سیستمونو او سافټ معلوماتو په محرمیت او دوام کې مرسته وکړي.

3.22. د معلوماتو (ډیټا) بیک اپ څارنه: په منظم ډول د مهمو معلوماتو (ډیټا) د خوندي کولو لپاره باید قوي بیک اپ سیستمونه عیار شي، او پدې برخه کې په منظم ډول د مهالویش مطابق د پوهنتون د ټولو اداري او علمي برخو معلومات بیک اپ شي او

همدارنګه د معلوماتو د لاسه ورکولو یا سیستم د ناکامۍ په صورت کې د معلوماتو د بیرته راګرځیدو لپاره باید پلانونه او د څارنې کړنلارې واضح شي، دا به د پوهنتون د معلوماتو په دوامداره ساتنه او ارزښت کې مهم رول ولوبوي.

4.22. امنیتي سیستمونو څارنه او ساتنه: د پوهنتون د معلوماتي تکنالوژۍ زیربنا او حساسو معلوماتو خوندي کولو لپاره قوي امنیتي تدابیر پلي کول او د یادو تدابیرو څارنه او ساتنه شامل دي، پدې کې د سیستمونو د مداخلې د کشف الې، د انټي ویروس سافټویرونه، د لاسرسي کنترولونه ، اور وژونکې الې شاملې دي، پدې برخه کې د کارکوونکو او محصلینو روزنه ترسره کول تر څو د احتمالي خطرونو په پیژندلو او په نښه کولو کې د هغوي پوهه لوړه او په منظمه او موثره توګه د اړونده تجهیزاتو او سیستمونو څارنه او ساتنه وکړي.

5.22. د معلوماتي تکنالوژۍ د شتمنیو لستونه: د معلوماتي تکنالوژۍ سرچینو په موثره توګه تعقیب او اداره کولو لپاره د شتمنیو مدیریت سیستمونه پلي کول شامل دي، تر څو د هارډویر او سافټویر شتمنیو تازه لیستونه د دوي د مشخصاتو، لکه د جنس نوم، سریال نمبر، ټاګ نمبر، د شتمنۍ نوعیت، موقیعت، د اعتبار نیټه، ارزښت او نور اړین معلومات شامل وي دا به د نویو کلونو او د څانګو لخوا د غوښتونکو توکو په صورت کې د شتمنیو په تخصیص کې مرسته وکړي.

6.22. د انټرنیټي سیستمونو څارنه: د معلوماتي تکنالوژۍ په برخه کې په پوهنتون کې د ټولو کارکوونکو، محصلینو، مهمو مرکزونو، کمپیوتر لیب او کتابتون په برخه کې چې انټرنیټ کاروي باید د انټرنیټ منظم حسابونه ترتیب او د اپلوډ او ډاونلوډ د حد او همدارنګه د سرعت د حد په اساس ورته ویش ترسره شي، او د انټرنیټ د ویش په صورت کې د کارونې هفته وار، میاشتینۍ، ربعه وار او کلنۍ مقایسوي راپورونه ترتیب شي، او د یادو راپورونو په صورت کې د لوړې کارونې په صورت کې د سلسله مراتبو په نظر کې نیولو سره اړونده کارمندانو ته خبر ورکړل شي.

7.22. د کارونکي سروې او فیډبیک: د معلوماتي تکنالوژۍ د خدماتو او سیستمونو په لړ کې د استادانو، کارمندانو او محصلینو څخه باید د رضایت سروې ګانې ترسره شي، تر څو د معلوماتي تکنالوژۍ خدماتو څخه د دوي رضایت اندازه شي او هغه ساحې وپیژندل شي چې پرمختګ ته اړتیا لري، دا ممکن د ډیټابیس، انلاین سیستمونو، ګروپي بحثونو، د شکایتونو او وړاندیزونو بکسونو او یا هم د ځانګړو فورمونو په وسیله ترسره شي.

8.22. د معیارونو سره پرتله: د پوهنتون د معلوماتي تکنالوژۍ وسایلو فعالیت د صنعت او د لوړو زده کړو وزارت د غوره کړنو او معیارونو سره پرتله کړئ، د کیفیت لوړونې معیارونه باید تعقیب او مطالعه شي او د پوهنتون د معلوماتي تکنالوژۍ سیستمونه باید د یادو معیارونو په اساس عیار او ترتیب شي او پدې برخه کې د معیارونو سره د پرتلې څارنه او نظارت ترسره شي.

درویشتمه ماده: د سرور او کیمرو خونې لپاره لارښوونې

په پوهنتون کې سرورخونه او د امنیتي کیمرو د کنترول خونه د معلوماتي تکنالوژۍ په برخه کې د پوهنتون د مهمو زیربناو څخه ده، سرور خونه د معلوماتي تکنالوژۍ په برخه کې د شبکې د تجهیزاتو او نورو معلوماتي سیستمونو، انلاین او (Local) سرورونو درلودونکې وي، او همدارنګه د امنیتي کیمرو خونه د څارنې، فوټیج د ثبت کولو لپاره کارول کیږي تر څو د امنیتي او معلوماتي ویډیوګانو د کلیپونو څخه په وروسته وخت کې د اړتیا پر اساس د ځانګړي میکانیزم په وسیله استفاده وشي، سرور خونې او امنیتي کیمرې د معلوماتي تکنالوژۍ زیربنا او د څارنې سیستمونو، امنیت، اعتبار، مسایلو ته رسیدګی، او د فعالیتونو د اغیزمنتیا ډاډمن کولو لپاره اړین دي، په پوهنتون کې د سرور خونې او امنیتي کیمرو لپاره لاندې لارښوونې وړاندې کیږي:

1. د سرور خونې او امنیتي کیمرو لپاره باید د پوهنتون په دننه کې یوه خوندي او په ټولو معیارونو برابره ساحه (اطاق) غوره شي.

2. د سرور او امنیتي کیمرو خونې ته باید یوازې مجاز او مسؤل کارمندانو په فزیکي ډول لاسرسي ولري، یادو خونو ته د داخلېدو منظم کنترول او د اجازت کارتونه ډیزاین او مختلف میکانیزمونه موجود وي.
3. په سرور خونه او امنیتي کیمرو خونه کې باید د اور وژنې او اضطراري حالاتو لوازم نصب وي تر څو د غیر مسؤلو اشخاصو د داخلېدو ، اور لګېدنې او نورو حالاتو کې مخنیوی ترسره شي.
4. په سرور خونه او امنیتي کیمرو خونه کې باید د مناسبې تودوخې، رطوبت او د وینټیلیشن سیستمونه عیار شي تر څو د تجهیزاتو غوره فعالیت یقیني او د زنګو او نورو خطراتو څخه مخنیوي وشي.
5. د اور وژنې اتومات او غیر اتومات سیستمونه باید عیار شي لکه د لوګي کشف کونکي (سینسرونه)، اور وژونکي او د اور وژنې اتوماتیک سیستمونه.
6. په سرور خونه کې د بریښنا د بیک اپ (UPS) سیستمونو او د بریښنا د توزیع واحدونو (PDUs) او د بریښنا د بې نظمۍ لپاره د سیستمونو عیارول تر څو د سرورونو او امنیتي کیمرو د فعالیت جریان ډاډمن شي.
7. په منظمه او مهالنۍ توګه د بیک اپ بریښنا سیستمونو ازموینه ترسره کړئ تر څو ډاډ ترلاسه شي چې د بریښنا د بندیدو پر مهال په سمه توګه کار کوي.
8. سرور خونو کې د کیبل مدیریت تخنیکونه باید وکارول شي لکه د کیبل ټرۍ، ریکونه او لیبلونه دا د شبکې د مزو د پاک ساتلو، ګډوډۍ کمولو، او د ستونزو په حل کولو کې مرسته کوي تر څو په اسانۍ سره حل شي.
9. د پوهنتون د شبکې زیربنا عمومي لارښود او نقشه باید ترتیب شي، څو پوهنتون ته د انټرنیټ او نورو شبکو د لینونو، سویچونو روټرونو او نورو معلوماتي تکنالوژۍ اړونده سیستمونو ځایونه او نقطې مشخصې وي.
10. د سرورونو او شبکې تجهیزاتو د فعالیت ډاډ حاصلولو لپاره د څارنې او نظارت تعقیبي سیستمونه رامینځته کول تر څو په سرورخونه کې د سیستمونو، د هوا فلټرونه (جالۍ او پکي) پاکول، د کیبلونو اتصال چیک کول او په هغه ځایونو کې چې د ترمیماتو اړتیا وي ترسره کول.
11. په سرور خونه کې د معلوماتو د بیک سیستمونه پلي کول، پدې کې ممکن د انلاین بیک (کلاوډ بیک اپ) او همدارنګه په فزیکي ډول په نورو سیستمونو کې د بیک اپ اخیستل شامل دي.
12. د سرور خونې دکارونې او لاسرسي لپاره د مختلفو پروسیجري اسنادو ساتنه لکه د شبکې ډیاګرامونه، د تجهیزاتو لستونه، د عادي کارونو او ستونزو حل کولو او ثبت کولو لپآره معیاري عملیاتي پروسیجرونه (SOPs).
13. د سرور خونې د پالیسیو، پروسیجرونو او امنیت غوره کړنو په اړه کارمندانو ته روزنه ورکول.
14. د څارنې فوټیج ذخیره کولو او اداره کولو لپاره وفق شوي شبکې ویډیو ریکارډر (DVR) یا د ویډیو مدیریت سافټویر (VMS) وکاروئ.
15. د قانوني او واک لرونکو اداراتو او د پوهنتون د پالیسیو او غوښتنو پر اساس باید لږ تر لږه ویډیوي ریکارډونه تر دریو میاشتو وساتل شي، او پدې جریان کې مهم او ارزښتناکه ویډیو کلیپونه باید په دوامداره توګه په محرم شکل وساتل شي.
16. په منظمه توګه کیمرې معاینه او ساتنه یې وشي، څو ډاډ ترلاسه شي چې کېمرې پاکې، په اړونده برخه متمرکزې او په غوره حالت کې دي.
17. د کېمرو د ساتنې، څارنې او د پېښو د عاجلو او عادي غبرګونونو او معلوماتو د ثبت او وړاندې کولو لپاره معیاري عملیاتي کړنلارې (SOPs) او پروسیجرونه رامینځته کول او کارول.
18. د پوهنتون د داخلي کارکوونکو او بهرنیو واک لرونکو اداراتو څخه د راغلو اشخاصو او معلوماتو د غوښتلو لپاره باید منظم فورمونه ډیزاین او د پوهنتون د باصلاحیته مسؤلو کارمندانو له لورې د تائیدۍ وروسته سرور خونې او امنیتي

کیمرو ته د معلوماتي تکنالوژۍ د مسؤلو کارمندانو لخوا لاسرسي پیدا او معلومات د معلوم پروسیجر له لارې ورکړل شي.

19. ستونزو د پېښېدو او د جنس د ورکیدو یا نورو موضوعاتو په وخت کې متضرره شخص باید تر (۲۴) ساعتونو پورې شکایت په اړونده مرجع کې درج کړي، وروسته له ټاکل شوي وخت اداره د ستونزې په لاسرسي او د جنس په لټون باندې مکلفه نه ده.
20. عارض شوی شخص به په شکایت کې د ورک شوي جنس یا ستونزې ډول، ځای،وخت او تاریخ ذکر کوي،چې د رسیدګۍ په وخت کې اساني رامنځته کړي.
21. متضرره شوی شخص دې د ورک شوي جنس یا ستونزې په اړه شکایت له اړونده مرجع سره شریک کړي،چې په رسمي ډول معلوماتي ټکنالوژۍ امریت ته د څېړلو لپاره وسپارل شي.
22. متضرره شوی شخص نشي کولای چې د ستونزې د پلټلو په اړه سرورخونې ته مستقیماً مراجعه وکړي.
23. موضوع باید د معلوماتي تکنالوژۍ آمریت د مسؤلو کارمندانو له لورې وڅېړل شي که اړتیا وه یاد عارض کوونکی یې هم ملتیا کولای شي او د څېړلو وروسته به یې نتیجه له اړونده مرجع سره شریکه شي.
24. معلوماتي ټکنالوژۍ امریت د سرورخونې مدیریت د ستونزې د پېښیدو او ورک شوي جنس په له منځه تللو نه دی مکلف البته په اړه یې د څېړلو مسؤلیت لري.
25. معلوماتي تکنالوژۍ آمریت باید د سرور خونې، امنیتي کېمرو د سرورونو، لینونو، کیبلونو، کیمرو او پدې برخه کې د ټولو تجهیزاتو څخه په میاشتینې ډول د ځانګړې چیک لست مطابق څارنه او نظارت ترسره کړي او راپورونه یې باید اداري او مالي چارو معاونیت سره په رسمي ډول شریک شي.

څلور ویشتمه ماده: د کمپیوتر لیب څخه د استفادې کړنلاره

په پوهنتون کې کمپیوتر لیب د محصلینو او څېړونکو استادانو لپاره د معلوماتي تکنالوژۍ د سیستمونو او انټرنیټ څخه د ګټې اخیستنې ارزښتناکه زیربناء او سرچینه ده، تر څو محصلین پکې د انټرنیټ او نورو زده کړو له لارې تخنیکي سرچینو ته لاسرسي پیدا کړي، دا په اصل کې د محصلینو د عملي کارونو او دندو ترسره کولو لپاره رامینځته شوی تر څو محصلین د نصابي او غیر نصابي او د ټولګي څخه بهر په مختلفو فعالیتونو او عملي کارونو کې ښکیل او همدارنګه د پوهنتون د دوهمې اصلي دندې چې څېړنه ده په صحیح شکل ترسره کړي، ددې لپاره چې د پوهنتون محصلین او کارکوونکي د کمپیوترلیب څخه په صحیح او مناسب ډول استفاده وکړي په لاندې ډول د کمپیوتر لیب څخه د ګټې اخیستنې څو لارښوونې او طرز العملونه وړاندې کیږي:

1.24. د قواعدو او اصولو سره اشنا کیدل: د پوهنتون د کمپیوتر لیب څخه د استفادې وړاندې دا اړینه ده چې ځان د کمپیوتر لیب د اصولو او قواعدو سره اشناء کړئ، پدې لارښوونو کې ممکن د سافټویرونو ډاونلوډ کولو محدودیتونه، ځینو ویب پاڼو ته لاسرسی، د تجهیزاتو ساتنه او یا هم په کمپیوتر لیب کې د مناسب چلند لارښوونې شاملې وي.

2.24. د کمپیوتر لیب اجازه: د کمپیوتر لیب د دوامداره او پرته د استاد د عملي کار څخه د کارونې لپاره باید د اجازې کارتونه ډیزاین او د معلوماتي تکنالوژۍ آمریت د مسؤلینو له لورې د ځانګړې ثبت کتاب په وسیله ورکړل شي، دا کولای شي چې د کمپیوتر لیب څخه د کاروونکو محصلینو په احصایه او د معلوماتو په ثبت کې مرسته وکړي.

3.24. د کمپیوتر لیب د کارونې وختونه: د کمپیوتر لیب لپاره باید د کارونې مختلف وختونه مشخص شي، تر څو مراجعه کوونکي او استادان خپل تدریسي او عملي زده کړو مهالویشونه په همغه ترتیب برابر کړي، پدې کې ممکن د محصلینو د تدریسي

مضامینو د عملي کارونو لپاره وخت، د عمومي کارونې لپاره ځانګړي شوي وختونه او یا هم د محصلینو او استادانو لپاره د جلا وختونو ترتیب موجود وي.

4.24. په کمپیوتر لیب کې شخصي توکي: ډاډ باید ترلاسه شي چې محصلین کمپیوتر لیب ته د ننوتلو د مخه خپل شخصي توکي، بیکونه، لپټاپ کمپیوترونه او نور توکي د توکو لپاره ټاکل شوي ځای کې پریږدي او بیا کمپیوترلیب ته داخل شی، دا به د کمپیوتر لیب د تجهیزاتو د ضایع کیدو یا ورکېدو په مخنیوي کې مرسته وکړي.

5.24. د نورو کارووونکو درناوی: کمپیوتر لیب د ټولو د استفادې شریک ځای دی نو دا مهمه ده چې د نورو کارووونکو حقوقو ته درناوی وشي او یو خاموش ، ارام او متمرکز چاپیریال وساتل شي، د ګډوډونکو فعالیتونو څخه ډډه وشي لکه په لوړ غږ موسیقي غږول، په لوړ غږ خبرې کول، یا د نامناسبې ژبې او الفاظو کارول.

6.24. خپل وخت مدیریت کول: خپل کار او ټاکل شوی وخت په منظم ډول مدیریت کړئ تر څو د مهالویش مطابق د نورو مراجعه کوونکو وخت ضایع نشي او همدارنګه تاسې ته د کمپیوتر لیب د کارونې څخه یو څه په لاس درشي، همدارنګه د کمپیوتر لیب په کمپیوترونو کې خپله شخصي (USB) مه داخلوئ او د سیستمونو د ترتیباتو (سیټینګ) مه تغیروئ.

7.24. د ستونزو راپور: که چیرته د کومې تخنیکي ستونزې سره مخ شئ، د تجهیزاتو خرابوالي، یا په کمپیوتر لیب کې کوم زیان رسونکي شیان وګورئ نو په سمدستي توګه د کمپیوتر لیب مسؤل او یا هم د معلوماتي تکنالوژی آمریت ته راپور ورکړئ، دا مرسته کوي او ډاډ ترلاسه کوي چې کمپیوتر لیب د ټولو کارووونکو لپاره په غوره کاري حالت کې پاتې کیږي.

8.24. د کمپیوترلیب عمومي طرز العمل: د پورته ټاکل شوو لویو برخوترځنګ د کمپیوترلیب د کارونې خاص،لنډ اصول او قواعد په لاندې ډول ذکر کیږي چې کمپیوتر لیب ته هر مراجعه کوونکی یې باید تعقیب او عملي کړي:

1. کمپیوټر خونې ته د داخلیدو په وخت کې هر محصل مکلف دی چې خپل نوم د کمپیوټر خونې څخه د استفادې د ثبت په کتاب کې راجستر کړي.
2. کمپیوټرخونې څخه ګټه اخیستونکی شخص باید د پوهنتون هویت کارت ولري.
3. په کمپیوټرلیب کې یو شخص د بل شخص د پوهنتون له هویت کارت څخه استفاده نشي کولای.
4. هر مراجعه کوونکی مکلف دی چې په کمپیوټرخونې کې له بې ځایه خبرو کولو څخه ډډه وکړي تر څو د نورو اشخاصو د وخت د ضایع کیدو سبب ونه ګرځي.
5. کمپیوټرلیب ته راتلونکی اشخاص مکلف دي چې په ټاکل شویو وختونو کې کمپیوټر خونې ته مراجعه وکړي.
6. مراجعه کوونکي مکلف دي چې په کمپیوټر خونې کې د نشه یي توکو له کارولو څخه ډډه وکړي.
7. کمپیوټر خونې ته د داخلیدو په وخت کې خپل بیګونه او نور لوازم مسؤل شخص ته وسپاري.
8. مراجعه کوونکی باید د کمپیوټر خونې نظم او ډیسپلین مراعت کړي او د تللو په وخت کې چوکۍ او نور لوازم خپل ځای کیښودل شي.
9. کمپیوټر خونې کې د ګرځنده ټیلیفون له استعمال او خبرو کولو څخه ډډه وشي، څو د نورو محصلینو د مزاحمت سبب ونه ګرځي.
10. مراجعه کوونکی په کمپیوټر خونه کې له یو درسي ساعت څخه د ډیر وخت تېرولو حق نلري.

پنځه ویشتمه ماده: په کتابتون کې د معلوماتي تکنالوژی کارونه

د پوهنتون په کتابتون کې د معلوماتي تکنالوژی د معلوماتي سرچینو او انلاین زده کړو په برخه کې د مؤثریت، لاسرسي او مدیریت لوړولو کې مهم رول لوبوي، د فزیکي (دودیز) کتابتونونو په نسبت په ننې عصر کې ډیجیتل کتابتونونو ته ډیره اړتیا

لیدل کیږي، څو د بریښنایي سرچینو پراخه لړی ته محصلین ، استادان او څیړونکي په اسانۍ سره لاسرسی وموميږي په لاندې ډول د پوهنتون په کتابتون کې د معلوماتي تکنالوژۍ عمومي لارښوونې واضح کیږي:

1.25. ډیجیتل کتلاګونه او انلاین ډیټابیسونه: د پوهنتون کتابتونونه د ډیجیتل کتلاګونو او انلاین ډیټابیسونو رامینځته کولو او ساتلو لپاره باید معلوماتي تکنالوژۍ وسایل وکاروي، دا پلیټ فارمونه کارووونکو ته اجازه ورکوي چې د بریښنایی سرچینو پراخه لړی وپلټي او لاسرسی ورته وموميږي ، لکه کتابونه، ژونالونه، مقالې او زده کړیزو اهدافو لپاره مختلف ډوله ملټي میډیا مواد، کارونکي کولای شي پرمختللي ویبسایټونه وپلټي او د زده کړو او عملي کارونو او کورنیو دندو لپاره ورڅخه استفاده وکړي.

2.25. د الکترونیکي منابعو مدیریت: د معلوماتي تکنالوژۍ سیستمونه د بریښنایی سرچینو په موثره توګه اداره کولو لپاره ځای پرځای کیږي، دې کې ډیجیتل سرچینو لکه (E-Books, E-Journals) او نور ډیټابیسونه ترلاسه کول، تنظیم کول، د لاسرسي جوازونه اخیستل او چمتو کول شامل دي همدارنګه د کتابتون کارمندانو لخوا د پوهنتون د ډیټابیس (ERP) سیستم په وسیله د فزیکي او بریښنایی کتابتون ټول سیستمونه باید د یاد سیستم په وسیله مدیریت او کنترول شي.

3.25. بریښنایی سرچینو ته د لیږې لاسرسی: معلوماتي تکنالوژۍ د پوهنتون کتابتونونو ته وړتیا ورکوي تر څو خپلو سرچینو ته د لیږې لاسرسي سیستمونه عیار کړي، محصلین، استادان او څېړونکي کولی شي ډیجیتل موادو ته له هرځای او هر وخت څخه د مشخصو اکاونټونو په درلودلو سره لاسرسي وموميږي او په دې برخه کې د خپلو زده کړیزو او څیړنیزو پروسو لپاره بریښنایی کتابونه، مقالې او نور ډیجیتل مواد ډاونلوډ کړي.

4.25. د بریښنایي زده کړو ځایونه او سیستمونه: معلوماتي تکنالوژي د پوهنتون په کتابتون کې د همکارۍ او پوهې شریکول اسانه کوي انلاین پلیټ فارمونه، لکه د بریښنایي زده کړو چاپیریال یا د زده کړو د مدیریت (LMS) سیستمونه دا ډاډمنوي چې د پوهنتون محصلین او استادان په ګروپي زده کړو او همدارنګه د نورو پوهنتونونو او څیړنیزو مراکزو سره مدغم شي، نو پدې برخه کې باید معلوماتي تکنالوژۍ آمریت د بریښنایي زده کړو ټول اړین سیستمونه رامینځته او د کارونې ډاډ یې ترلاسه شي.

شپږ ویشتمه ماده: د بریښنایي زده کړو او معلوماتي تکنالوژۍ ادغام

په اوسني ډیجیتل عصر کې د بریښایي زده کړې او معلوماتي تکنالوژۍ ادغام د زده کړې په ډګر کې د بدلون لوی ځواک ګرځیدلی، په ټوله نړۍ کې تحصیلي بنسټونه د زده کړې تجربې ته د وده ورکولو، د پایلو پربسنټ د ولاړو زده کړو معیارونو، زده کړو ته د لاسرسي پراخولو، او د زده کړو په برخه کې د تکنالوژۍ نویو غوښتنو ته د محصلینو چمتو کولو لپاره کارول کیږي، دا ادغام د معلوماتي تکنالوژۍ د متحرک بدلون او متقابل تعلیمي او تحصیلي چاپیریال رامینځته کولو لپاره د انلاین زده کړو پلیټ فارمونو، ملټي میډیا سرچینو او په اړونده برخو کې د همکارۍ وسیلو د ځواک ترکیب دی، دا محصلینو ته وړتیا ورکوي، څو د وخت او ځای خنډونه د زده کړو په ډګر کې مات کړي او د هر ځای څخه په هر وخت کې خپلو زده کړیزو اهدافو ته ورسیږي، د معلوماتي تکنالوژۍ او بریښنایي زده کړو د ادغام (یوځای) کولو لپاره لاندې لارښونې باید په پام کې ونیول شي:

1.26. زیربناوې او سرچینې

1. د پوهنتون په ټول داخلي اداري او تدریسي چاپیریال او ټولګیو کې د باور وړ انټرنیټي سهولتونه (اتصال) ډاډ ترلاسه کول.
2. د اړینو هارډویر او سافټویر سره سمبال کمپیوټر لیبونو تنظیمول.
3. د انلاین زده کړو پلیټ فارمونو او سرچینو ته لاسرسی چمتو کول.

2.26. د استادانو رزونه او ملاتړ

1. د اړونده پوهنځيو استادانو لپاره د روزنې برنامې وړاندې کول تر څو دوي د بريښنايي زده کړو وسيلو، پلیټ فارمونو او لابرېښوونو سره اشنا شي.
2. دوامداره ملاتړ او انلاين زده کړو سرچينې چمتو کول تر څو استادانو سره مرسته وکړي چې تکنالوژي د دوي په تدريسي بهير کې مدغم شي.
3. استادان بايد وهڅول شي چې د بريښنايي زده کړو مختلف تخنيکونه او ستراتيژيانې زده او پلي کړي.

3.26. د نصاب پراختيا او ډيزاين

1. هغه مفردات يا ماډلونه بايد وپيژندل شي چې په موثره توګه د بريښنايي زده کړو له لارې وړاندې کيدی شي.
2. د زده کړې پايلو (پايلو پربنسټ زده کړې) د ارزونې ميتودونو او د بريښنايي زده کړو فعاليتونو ترمنځ سمون او ورته والي ډاډمن کړئ.
3. د انلاين زده کړو په برخه کې داسې مفردات ډيزاين کول چې ملټي ميډيا عناصر او ګډ فعاليتونه پکې شامل وي.

4.26. د بريښنايي زده کړو پلیټ فارمونه او وسيلې

1. د زده کړې مديريت سيستم (LMS) غوره کول او تطبيق يې کول په هغه صورت کې چې د پوهنتون زده کړيزې اړتياوې او اهداف پوره کړي.
2. د (LMS) او نورو بريښنايی زده کړو وسيلو کارولو په اړه استادانو او محصلينو دواړو لپاره روزنه او تخنيکي ملاتړ چمتو کول.
3. د زده کړو تجربو ته وده ورکولو لپاره د اضافي وسيلو کارول لکه د ويډيو کنفرانس پلیټ فارمونه، انلاين سيستمونه او وسيلې او داسې نور بايد وپلټل شي او تطبيق شي.

5.26. د محصلينو ملاتړ او ښکيلتيا

1. محصلين د بريښنايي زده کړو چاپيريال او وسيلو سره اشنا کول.
2. محصلينو لپاره تخنيکي ملاتړ او د ستونزو حل کولو مرستې چمتو کول تر څو د بريښنايی زده کړې پلیټ فارمونو يا وسيلو په کارونه کې د ستونزو سره مخ نشي.
3. د بريښنالیک، چټ، ويډيو کنفرانسونو له لارې د استادانو او محصلينو ترمنځ د ارتباطاتو هڅول او د ګروپي بحثونو لپاره زمينه برابرول.

6.26. ارزونه او نظرونه

1. د ارزونې ميتودونه ډيزاين کول چې د بريښنايي زده کړو فارمټ سره سمون ولري لکه انلاين پوښتنې، فعاليتونه او بحثونه.
2. په (LMS) کې محصلينو ته د نمراتو اعلان، درجه بندی او همدارنګه د محصلينو د نظرياتو او پشنهاداتو لپاره د سيستمونو رامينځته کول او تطبيقول شامل دي.

7.26. ارزونه او دوامداره پرمختګ

په منظمه توګه د سروې، د معلوماتو تحليل او د محصلينو د نظرياتو له لارې د بريښنايي زده کړو او نوښتونو د اغيزمنتوب لپاره ارزونه ترسره کول.

راټول شوي فيډبيکونه او معلومات ددې لپاره کارول تر څو د پرمختګ لپاره ساحې وپيژندل شي او د بريښنايی زده کړو تګلارو کې اړين اصلاحات رامينځته او پلي شي.

د نويو وسيلو او ستراتيژيو د پلټنې او يوځای کولو لپاره د بريښنايي زده کړو او معلوماتي تکنالوژی په برخه کې د وروستيو پرمختګونو څخه ځان خبر، تازه او په خپلو سيستمونو کې يې تطبيق کړئ.

اوه ويشتمه ماده: د معلوماتي تکنالوژی راپور ورکونه

د پوهنتون معلوماتي تکنالوژی (IT) آمريت کې د داخلي او بهرني راپور ورکولو سيستمونه د معلوماتو په موثره توګه اداره کولو او خبرو اترو او د کارونو د تعقيب په برخه کې مهم رول لوبوي، د راپور ورکونې دا سيستمونه ډاډ ترلاسه کوي چې اړونده معلومات راټول شوي، تحليل شوي او د مناسبو څانګو او بهرنيو مربوطه او واک لرونکې اداري سره شريک شوي، په لاندې

ډول د معلوماتي تکنالوژی په برخه کې د آمریت اړونده کارمندان مکلف دي تر څو د ستونزو او معلوماتو نوعیت ته په کتو سره ورځني، هفته وار، میاشتیني، ربعه وار کلني او همدارنګه د ځانګړو پېښو او معلوماتو په اړه ځانګړي راپورونه چمتو او اړونده برخو ته واستوي.

1.27. د پېښو راپور ورکول: دمعلوماتي تکنالوژی کارمندان باید د داخلي راپور ورکولو سیستم له لارې رامینځته شوې پېښې او ستونزې باید د ځانګړو پروسیجر پاڼو له لارې راپور کړې لکه د سیستم ناکامي، د شبکې نه وصلیدل، د تجهیزاتو د ترمیم اړتیا، امنیتي سرغړونې او داسې نور.

2.27. د انټرنیټ د کنترول راپور: په میاشتیني ډول د انټرنیټي سیستمونو د کنترول او نظارت ځانګړي راپورونه چمتو کول اداري او مالي چارو معاونیت ته استول، په راپور کې باید د هر کارونکي معلومات، د ډاونلوډ او اپلوډ مقدار او همدارنګه د میاشتې په جریان کې د پالیسی څخه د سرغړونو په صورت کې د غیر اخلاقي سایټونو کارونه باید راپور شي.

3.27. د معلوماتي سیستمونو د نظارت راپور: د معلوماتي سیستمونو د څارنې او نظارت راپورونه باید په ربعوار ډول ترتیب او معاونیت ته واستول شي، په راپور کې باید د سیستمونو، وسایلو، تجهیزاتو د صحت او عدم صحت په اړه د ځانګړي شوي چیک لست له مخې څارنه ترسره او راپورونه یې له شواهدو سره ترتیب شي.

4.27. د ډیټابیس د ارزونو او تطبیق راپور: د پوهنتون د ډیټابیس د ښه او مؤثر تطبیق په لړ کې ځانګړي چیک لستونه جوړول او د کال په جریان کې دوه ځلې د یادو چیک لستونو پر اساس د ټولو برخو ارزونه ترسره کول او د تطبیق او عدم تطبیق مقایسوي راپورونه ترتیب او اداري شورا ته باید وړاندې شي.

5.27. د پوهنتون د ویبسایټ د ارزونو او تطبیق راپور: د پوهنتون د ویبسایټ د اړونده دوامداره تازه کیدونکو برخو او دایمي برخو په تعقیب ځانګړي چیک لستونه جوړول او د هغې پر مټ ارزونه ترسره کول او د تطبیق او عدم تطبیق مقایسوي راپورونه د معلوماتو او څانګو په تفکیک برابرول او اداري شورا ته وړاندې کول.

6.27. د کمپیوترلیب د کارونې راپورونه: د پوهنتون د عمومي کمپوتر لیب او یا هم د بریښنایي زده کړو د اړونده کمپیوترونو د کارونې په لړ کې باید ځانګړي د ثبت کتابونه ترتیب او په ورځني ډول تعقیب او راپورونه یې په ربعوار ډول د احصایوي معلوماتو او مقایسوي ګرافونو په تفکیک ترتیب او اړونده خواوو ته واستول شي.

7.27. د معلوماتي تکنالوژی په اړه د فیډبیک راپور: د معلوماتي تکنالوژی مسؤلین باید په اړونده برخه کې د خدماتو د ترسراوي په هکله په کال کې دوه ځلې د ځانګړو انلاین او یا هم په فزیکي ډول د پوښتنپاڼو له طریقه سروې ګانې ترسره او د هغې تحلیلي او مقایسوي راپورونه ترتیب او اداري او مالي چارو معاونیت ته یې واستوي.

8.27. په امنیتي کیمرو کې د ستونزو د کشف راپور: د پوهنتون په داخل او خوا او شاه چاپیریال کې د امنیتي کیمرو په وسیله کشف شویو پېښو او ستونزو کلني راپورونه باید د کیمرې د موقعیت، د نوعیت، نیټې، وخت، د پېښې تفصیل او انځوریزو شواهدو پر اساس کلني توحیدي راپور ترتیب او اداري او مالي چارو معاونیت ته واستول شي.

9.27. کارمندانو ته ګروپي او انفرادي روزنو راپور: په منځني او کلني ډول د پوهنتون د برحاله او نویو کارمندانو او همدارنګه محصلینو ته د معلوماتي تکنالوژی په برخه کې د هر ډول ګروپي او یا انفرادي ترینګونو او روزنو توحیدي راپورونه باید ترتیب او د پوهنتون تضمین کیفیت او اداري او مالي چارو معاونیت ته واستول شي.

10.27. د ستراتیژیک پلان لپاره د معلوماتي تکنالوژی د فعالیتونو راپور: په یو مشخص شوي او د ستراتیژیک پلان د غوښتنو مطابق د هر کال په جریان کې په پوهنتون کې د ستراتیژیک پلان په تعقیب د معلوماتي تکنالوژی په برخه کې د فعالیتونو، انکشافاتو او نوښتونو راپور باید ترتیب او اداري او مالي چارو معاونیت او پلان او پالیسی کمیټې ته واستول شي.

اته ویشتمه ماده: د پالیسی اړیني ضمیمې

1. د معلوماتي تکنالوژی د خدماتو د غوښتنې فورم

2. په (ERP) ډیټابیس سیستم کې د واک ورکولو فورم
3. اړونده څانګو ته د معلوماتي تکنالوژۍ په برخه کې د خدماتو د ترسراوي رسید فورم
4. په ډیټابیس سیستم کې د استادانو لخوا د درسي موادو د اپلوډ چیک لست
5. د معلوماتي تکنالوژۍ د اړونده سیستمونو د نظارت چیک لست.
6. د سرور خونې (امنیتي کیمرو) د معلوماتو د غوښتنې فورم
7. د اړونده څانګو څخه د ډیټا (معلوماتو) د بیک اپ رسید فورم
8. د ډیټابیس د اړونده برخو د ارزونو لپاره معیاري چیک لستونه
9. نویو کارکوونکو ته د معلوماتي تکنالوژۍ د انفرادي ترېننګ د رسید فورم
10. د کارمندانو د دندې د پیل او پای لپاره د معلوماتي تکنالوژۍ د وسایلو سپارلو او تسلیمولو فورم
11. د معلوماتي تکنالوژۍ د خدماتو وړاندې کولو په لړ کې د کارکوونکو د فیډبیک فورم
12. د معلوماتي تکنالوژۍ په برخه کې معیاري قرارداد فورم
13. د پوهنتون د انټرنیټ د ډاونلوډ او اپلوډ د ورځنۍ ثبت فورم
14. د محصلینو د خبرتیاو استولو لپاره د څانګړي فورم
15. د پوهنتون د امنیتي کیمرو څخه د نظارت چیک لست
16. د امنیتي کیمرو په برخه کې د پیښو د کشف راپور کولو فورم
17. د انټرنیټ د ډاونلوډ او اپلوډ میاشتینۍ راپور فورم
18. د معلوماتي تکنالوژۍ د وسایلو او تجهیزاتو د ثبت او انتقال فورم
19. د کمپیوټر لیب څخه د استفادې څانګړی کړنلاره
20. د سرور خونې او امنیتي کیمرو ته د لاسرسي څانګړی فورم

نهه ویشتمه ماده: د پالیسۍ تائیدي

د معلوماتي تکنالوژۍ د اسانتیاوو د ساتنې، پاملرنې او مناسبې استفادې طرزالعمل د معلوماتي تکنالوژۍ چارو د تنظیم په موخه د (۲۹) مادو او اړونده فرعي عنوانونو کې ترتیب شوه، او د پلان او پالیسۍ کمیټې په (۲) ګڼه (۱۴۰۵/۰۲/۲۲) نیټې مجلس کې د بحث وروسته تائید او د عملي کیدو وړ ده.

د معلوماتي تکنالوژۍ پالیسي (لارښود) د اداري او مالي چارو معاونیت په چوکاټ کې د معلوماتي تکنالوژۍ د منظم پرمخ وړلو لپاره د (۲۹) مادو او اړونده فرعي عنوانونو کې ترتیب شوه، او د علمي شورا په (۲) ګڼه (۱۴۰۵/۰۲/۵۲۹) نیټې شورا کې د بحث وروسته تائید او د عملي کیدو وړ ده.

ترتیب: د معلوماتي تکنالوژۍ آمر
صدیق الله عادل

تائید: پوهنتون رئیس
عبدالحمید سیرت