საინფორმაციო ტექნოლოგიური პროცესების უწყვეტობის გეგმა

შინაარსი

IT პროცესების უწყვეტობის გეგმა

IT პროცესების უწყვეტობის მიზანი და გამოყენების ფარგლები

მიზანი: IT პროცესების უწყვეტობის გეგმის მიზანია უზრუნველყოს ვებსტერ უნივერსიტეტი, ინკ.-ის ფილიალი საქართველოში (შემდგომში - ფილიალი) კრიტიკული IT სისტემების, აპლიკაციებისა და მონაცემების შეუფერხებელი ხელმისაწვდომობა და ფუნქციონირება ნებისმიერი ინციდენტის ან კატასტროფის შემთხვევაში.

ეს გეგმა მიზნად ისახავს მინიმუმამდე დაიყვანოს ინციდენტების გავლენა ფილიალის ოპერაციებზე, დაიცვას ღირებული ინფორმაცია და შეინარჩუნოს აუცილებელი IT სერვისები ფაკულტეტის, პერსონალისა და სტუდენტებისთვის.

ფარგლები: IT პროცესების უწყვეტობის გეგმა მოიცავს ფილიალის IT ინფრასტრუქტურის ყველა ასპექტს, მათ შორის აპარატურას, პროგრამულ უზრუნველყოფას, მონაცემთა ცენტრებს, ქსელურ ინფრასტრუქტურას და IT პერსონალს. ის მოიცავს პოტენციური საფრთხეების ფართო სპექტრს, როგორიცაა ბუნებრივი კატასტროფები, კიბერშეტევები, აღჭურვილობის გაუმართაობა და სხვა გაუთვალისწინებელი მოვლენები, რამაც შეიძლება ზიანი მიაყენოს IT სერვისებს. გეგმა ასახავს ყოვლისმომცველ სტრატეგიებს, რეაგირების პროცედურებს და აღდგენის მექანიზმებს სხვადასხვა დონის შეფერხების აღმოსაფხვრელად და პრიორიტეტული IT სისტემების აღდგენის მიზნით.

ფილიალის IT ინფრასტრუქტურისა და კრიტიკული სისტემების მიმოხილვა

ფილიალის IT ინფრასტრუქტურა არის რთული ეკოსისტემა, რომელიც მხარს უჭერს სხვადასხვა აკადემიურ, ადმინისტრაციულ და კვლევით საქმიანობას. იგი მოიცავს შემდეგ კრიტიკულ კომპონენტებს:

1. **მონაცემთა ცენტრი:** უნივერსიტეტს აქვს ცენტრალიზებული მონაცემთა ცენტრები, სადაც განთავსებულია სერვერები და აპლიკაციების, მონაცემთა ბაზებისა და აკადემიური რესურსების შენახვის სისტემები.

2. **ქსელის ინფრასტრუქტურა:** ძლიერი ქსელის ინფრასტრუქტურა აკავშირებს ყველა დაინტერესებულ მხარეს. მასში შედის სადენიანი და უკაბელო ქსელები, მარშრუტიზატორები, გადამრთველები და დამცავი პროგრამები და VPN. სადენიანი ქსელი დაყოფილია აკადემიურ და პერსონალურ დანაყოფებად, წვდომა რეგულირდება მომხმარებლის დონის მიხედვით.

3. **აკადემიური აპლიკაციები:**

- CX (მხარდაჭერით Jenzabar) არის სისტემა, რომელიც მხარს უჭერს სტუდენტურ და ადმინისტრაციულ სერვისებს, როგორიცაა კურსის რეგისტრაცია, კურსის ინფორმაციის ჩვენება და აკადემიური ჩანაწერების ნახვა. CX ხელმისაწვდომია გლობალურად ყველა ფაკულტეტის, პერსონალისა და სტუდენტებისთვის. CX მოცულობა და გამოყენება რეგულარულად კონტროლდება.

- Connections (მხარდაჭერილია Microsoft Sharepoint-ის მიერ) არის ვებ პორტალი, წვდომის ერთი წერტილი ბევრ ონლაინ სერვისზე. ის აერთიანებს ონლაინ კურსებს, ონლაინ რეგისტრაციას, კლასების შეყვანას, გადასახადის შესახებ ინფორმაციას და სხვას ერთ ვებ ინტერფეისში, რომელზე წვდომა შეიძლება ნებისმიერი ინტერნეტის მქონე მოწყობილობიდან.

- კავშირები ხელმისაწვდომია გლობალურად ყველა ფაკულტეტის, პერსონალისა და სტუდენტისთვის.

- კავშირების სიმძლავრე და გამოყენება რეგულარულად კონტროლდება.

- LMS „WorldClassRoom“ (მხარდაჭერილია სწავლის მართვის სისტემით Canvas by Instructure) არის პორტალი, რომელიც გამოიყენება Webster-ის ყველა ონლაინ კურსებისთვის. იგი მოიცავს ბევრ ინსტრუმენტს და მახასიათებელს, რომლებიც მომხმარებელს ხელს უწყობს გახადოს ონლაინ სწავლის გამოცდილება ეფექტური და ინტუიციური.

- WorldClassroom ხელმისაწვდომია გლობალურად ყველა ფაკულტეტისა და სტუდენტებისთვის

- WorldClassroom-ის მოცულობა და გამოყენება რეგულარულად კონტროლდება. WorlClassroom არის ზომის, რათა მხარი დაუჭიროს ფილიალის მიმდინარე და მომავალ ზრდას

4. **ადმინისტრაციული სისტემები:** ეს სისტემები მართავენ სტუდენტთა ჩანაწერებს, ფინანსურ ტრანზაქციებს, ადამიანურ რესურსებს, სახელფასო და სხვა ადმინისტრაციულ ფუნქციებს:

- ფაკულტეტი და პერსონალი CX (მხარდაჭერილია Jenzabar მიერ) არის სისტემა, რომელიც მხარს უჭერს ყველა ადმინისტრაციულ მომსახურებას, როგორიცაა კურსის რეგისტრაცია, კურსის ინფორმაციის ჩვენება და აკადემიური ჩანაწერების ნახვა. CX ხელმისაწვდომია გლობალურად ყველა ფაკულტეტისა და პერსონალისთვის. CX მოცულობა და გამოყენება რეგულარულად კონტროლდება.

- Connections (მხარდაჭერილია Microsoft Sharepoint-ის მიერ) არის ვებ პორტალი, წვდომის ერთი წერტილი ბევრ ონლაინ სერვისზე. ის აერთიანებს ონლაინ კურსებს, ონლაინ რეგისტრაციას, კლასების შეყვანას, გადასახადების შესახებ ინფორმაციას და სხვას ერთ ვებ ინტერფეისში, რომელზე წვდომა შეიძლება ნებისმიერი ინტერნეტის მქონე მოწყობილობიდან.

- კავშირები ხელმისაწვდომია გლობალურად ყველა ფაკულტეტისა და პერსონალისთვის.

- კავშირების სიმძლავრე და გამოყენება რეგულარულად კონტროლდება.

5. **ელექტრონული ფოსტა და თანამშრომლობის ინსტრუმენტები:** უნივერსიტეტის მასშტაბით ელ.ფოსტის სერვისები და თანამშრომლობის პლატფორმები ხელს უწყობს კომუნიკაციას და ინფორმაციის გაზიარებას ფაკულტეტებს, პერსონალსა და სტუდენტებს შორის. Webster University Georgia-ს ელ.ფოსტის ყველა სერვისი წარმოებს Microsoft Outlook-ით.

6. **ვებგვერდი და ონლაინ სერვისები:** ფილიალის ოფიციალური ვებგვერდი www.webster.edu.ge, რომელიც უზრუნველყოფს ინფორმაციას, რესურსებს და მომსახურებას ფართო საზოგადოებისთვის ყველა სერვისი უზრუნველყოფილია წვდომის რეგულირებადი ინტრანეტით: “Connections Portal”.

ძირითადი დაინტერესებული მხარეები და მათი როლები უწყვეტობის პროცესში

1. **IT ლიდერთა გუნდი:** ფილიალის საინფორმაციო ტექნოლოგიების გუნდში შედგება ფილიალის ინფორმაციული ტექნოლოგიების მენეჯერის და აშშ და გლობალური სათაო ოფისის გუნდისაგან. ისინი პასუხისმგებელნი არიან საერთო გეგმის მართვასა და კოორდინაციაზე. გეგმას ამტკიცებს რექტორი.

2. **IT უწყვეტობის დაგეგმვის კომიტეტი:** ფილიალს აქვს ინფორმაციული ტექნოლოგიების განვითარებისა და უწყვეტობის გეგმა. სხვადასხვა სტრუქტურული ერთეულების წარმომადგენლების შემადგენლობით, ისინი თანამშრომლობენ უწყვეტობის გეგმის შემუშავებაში, განხილვასა და განახლებაში.

3. **ინციდენტზე რეაგირების ჯგუფი:** ფილიალში დასაქმებულია ინფორმაციული ტექნოლოგიების მენეჯერი, რომელიც ინციდენტების შემთხვევაში იწყებს რეაგირების პროცედურებს და კოორდინაციას უწევს აღდგენის პროცესს.

4. **პერსონალი:** ისინი ასრულებენ გადამწყვეტ როლს უწყვეტობის გეგმის დაცვაში, ინციდენტების მოხსენებაში და პროცედურების დაცვაში მინიმალური შეფერხების უზრუნველსაყოფად.

პოტენციური IT შეფერხებებისა და საფრთხეების იდენტიფიცირება

1. **სტიქიური უბედურებები:**

- მიწისძვრებმა, ქარიშხლებმა, წყალდიდობებმა, ტყის ხანძრებმა და სხვა სტიქიურმა კატასტროფებმა შეიძლება გამოიწვიოს ფიზიკური დაზიანება მონაცემთა ცენტრებისთვის, ქსელის ინფრასტრუქტურისა და IT აღჭურვილობისთვის.

2. **კიბერშეტევები:**

- ვირუსულმა პროგრამამ, ransomware პროგრამამ, DDoS შეტევებმა და ჰაკერების მცდელობებმა შეიძლება დაარღვიოს მონაცემთა მთლიანობა, დაარღვიოს IT სერვისები და გამოიწვიოს მონაცემთა დაზიანება.

3. **ელექტროენერგიის გათიშვა:**

- ელექტრომომარაგებამ, ქსელის პრობლემებმა ან ინფრასტრუქტურის დაზიანებამ შეიძლება გამოიწვიოს ელექტროენერგიის გათიშვა, ზეგავლენა იქონიოს კრიტიკულ IT სისტემებზე და გამოიწვიოს შეფერხება.

4. **აპარატურის გაუმართაობა:**

- კომპონენტები, როგორიცაა მყარი დისკები, კვების წყაროები ან ქსელის მოწყობილობები, შეიძლება მოულოდნელად გაფუჭდეს, რაც გამოიწვევს სერვისის შეფერხებას და მონაცემთა დაკარგვას.

5. **ადამიანური შეცდომები:**

- პერსონალის მიერ მონაცემების შემთხვევით წაშლამ, არასწორმა კონფიგურაციამ და ოპერაციულმა შეცდომებმა შეიძლება გამოიწვიოს სერვისის შეწყვეტა და მონაცემთა გაფუჭება.

6. **პროგრამული უზრუნველყოფის ხარვეზები:**

- დაუმუშავებელი ან მოძველებული პროგრამული უზრუნველყოფა შეიძლება შეიცავდეს მოწყვლადობას, რომელიც შეიძლება გამოიყენონ თავდამსხმელებმა, პოტენციურად შეაფერხოს სერვისები ან დააზიანოს მონაცემები.

7. **ტელეკომუნიკაციის გაუმართაობა:**

- ინტერნეტის ან სატელეკომუნიკაციო სერვისების შეწყვეტამ შეიძლება გავლენა მოახდინოს ონლაინ სწავლაზე, კომუნიკაციაზე და ღრუბელზე დაფუძნებულ რესურსებზე წვდომაზე.

8. **მიწოდების ჯაჭვის შეფერხებები:**

- კრიტიკული ტექნიკის ან პროგრამული კომპონენტების მესამე მხარის მომწოდებლებზე დამოკიდებულებამ შეიძლება გამოიწვიოს შეფერხებები, თუ მიწოდების ჯაჭვი შეწყდება.

9. **სოციალური ინჟინერია:**

- ფიშინგის, პრეტექსტინგის და სოციალური ინჟინერიის სხვა ტექნიკის გამოყენება შესაძლებელია სისტემებსა და სენსიტიურ მონაცემებზე არაავტორიზებული წვდომის მოსაპოვებლად.

10. **Malicious Insiders:**

- პრივილეგირებული წვდომის მქონე უკმაყოფილო თანამშრომლებმა ან სტუდენტებმა შეიძლება განზრახ გამოიწვიოს შეფერხება ან სხვაგვარი დაზიანება.

ზემოქმედების ანალიზი თითოეული გამოვლენილი რისკისთვის

1. **სტიქიური უბედურებები:**

- გავლენა: გახანგრძლივებული დრო, მონაცემთა დაკარგვა, აკადემიური აქტივობების შეფერხება, დავალებების დაგვიანებული წარდგენა და ფილიალის დროებითი დახურვა.

2. **კიბერშეტევები:**

- გავლენა: სენსიტიური მონაცემების დარღვევა (სტუდენტური ჩანაწერები, კვლევის შედეგები), ინტელექტუალური საკუთრების დაკარგვა, ფინანსური ზარალი გამოსასყიდის გამო და რეპუტაციის დაზიანება.

3. **ელექტროენერგიის გათიშვა:**

- გავლენა: IT სერვისების სრული შეწყვეტა, ონლაინ გაკვეთილების შეჩერება, ონლაინ რესურსებზე წვდომის შეზღუდვა და მონაცემთა პოტენციური დარღვევა.

4. **აპარატურის გაუმართაობა:**

- გავლენა: შეფერხების დრო, დაზიანებულ აპარატურაზე შენახული მონაცემების დაკარგვა და კონკრეტული სერვისების ან აპლიკაციების შეფერხება.

5. **ადამიანური შეცდომები:**

- გავლენა: მონაცემთა დაკარგვა, შეფერხების დრო, კრიტიკული სერვისების დროებითი მიუწვდომლობა და სენსიტიური ინფორმაციის პოტენციური კომპრომისი.

6. **პროგრამული უზრუნველყოფის ხარვეზები:**

- ზემოქმედება: მოწყვლადობის ათვისება, რაც იწვევს არაავტორიზებული წვდომას, მონაცემთა გარღვევას და სერვისების შეფერხებას.

7. **ტელეკომუნიკაციის გაუმართაობა:**

- ზემოქმედება: შეზღუდულია ან არ არის წვდომა ონლაინ რესურსებზე, კომუნიკაციის შეფერხება და აკადემიური აქტივობების შეფერხება.

8. მიწოდების ჯაჭვის შეფერხებები:

- გავლენა: მნიშვნელოვანი IT კომპონენტების დაგვიანებული შესყიდვა, რაც იწვევს გახანგრძლივებულ მუშაობას და პოტენციურად გაზრდილ ხარჯებს სასწრაფო ჩანაცვლებისთვის.

9. სოციალური ინჟინერია:

- გავლენა: სისტემებზე არაავტორიზებული წვდომა, გატეხილი ანგარიშები და მონაცემთა პოტენციური დარღვევა.

10. Malicious Insiders:

- გავლენა: IT სისტემების საბოტაჟი, მონაცემთა გარღვევა და კრიტიკული სერვისების შეფერხება.

საფუძვლიანი ზემოქმედების ანალიზის ჩატარება საშუალებას აძლევს ფილიალს პრიორიტეტულად გამოყოს რისკის შერბილების ძალისხმევა და გამოყოს რესურსები ყველაზე კრიტიკულ საკითხებზე. ის ასევე იძლევა შესაბამისი რეაგირებისა და აღდგენის გეგმების შემუშავებას, რომელიც მორგებულია თითოეულ გამოვლენილ საფრთხის პოტენციურ შედეგებზე.

იდენტიფიცირება კრიტიკული IT სისტემები, აპლიკაციები და მონაცემები, რომლებიც საჭიროა ფილიალის არსებითი ფუნქციებისთვის. პრიორიტეტული IT აქტივები მათი გავლენისა და RTOs (Recovery Time Objectives) და RPOs (Recovery Point Objectives) საფუძველზე.

კრიტიკული IT სისტემების, აპლიკაციებისა და მონაცემების იდენტიფიცირება გადამწყვეტია IT შეფერხების დროს აღდგენის ძალისხმევის პრიორიტეტისათვის. ეს

აქტივები აუცილებელია ფილიალისთვის, რომ განაგრძოს თავისი ძირითადი ფუნქციები და შეინარჩუნოს ბიზნესის უწყვეტობა. აქ მოცემულია რამდენიმე მაგალითი:

IT აქტივების პრიორიტეტიზაცია RTO-სა და RPO-ებზე დაყრდნობით:

აღდგენის დროის მიზანი (RTO): სისტემის ან აპლიკაციის შეფერხების მაქსიმალური დასაშვები დრო, სანამ ის აღდგება და განაახლებს ფუნქციონირებას.

აღდგენის წერტილის მიზანი (RPO): მონაცემთა მაქსიმალური დასაშვები დაკარგვა, კერძოდ, რამდენი მონაცემი შეიძლება დაიკარგოს მანამ, სანამ ის მნიშვნელოვნად იმოქმედებს ფილიალის ოპერაციებზე.

აღდგენის პრიორიტეტი ჩვეულებრივ ენიჭება თითოეული აქტივის, RTO და RPO კრიტიკულობის მიხედვით. ქვემოთ მოცემულია შემოთავაზებული პრიორიტეტი:

1. დონე 1 - მაღალი პრიორიტეტი:

- LMS: RTO - საათებში, RPO - მონაცემთა მინიმალური დაკარგვა (წუთები თუ შესაძლებელია)
- SIS: RTO - საათებში, RPO - მონაცემთა მინიმალური დაკარგვა (წუთები თუ შესაძლებელია)
- ელ.ფოსტისა და საკომუნიკაციო სერვისები: RTO - რამდენიმე საათში, RPO - მონაცემთა მინიმალური დაკარგვა (წუთები თუ შესაძლებელია)

2. მე-2 დონე - საშუალო პრიორიტეტი:

- ფინანსური მართვის სისტემა: RTO - 24 საათის განმავლობაში, RPO - მონაცემთა მინიმალური დაკარგვა (საათი თუ შესაძლებელია)

- ადამიანური რესურსების მართვის სისტემა: RTO - 24 საათის განმავლობაში, RPO - მონაცემთა მინიმალური დაკარგვა (საათი თუ შესაძლებელია)
- კვლევის მონაცემთა ბაზები და აპლიკაციები: RTO - 24 საათის განმავლობაში, RPO - მონაცემთა მინიმალური დაკარგვა (საათი თუ შესაძლებელია)

3. მე-3 დონე - ქვედა პრიორიტეტი:

- ბიბლიოთეკის მართვის სისტემა: RTO - 48 საათის განმავლობაში, RPO - მონაცემთა მინიმალური დაკარგვა (საათი თუ შესაძლებელია)
- ონლაინ თანამშრომლობის ინსტრუმენტები: RTO - 48 საათის განმავლობაში, RPO - მონაცემთა მინიმალური დაკარგვა (საათი თუ შესაძლებელია)
- დაშვებისა და ჩარიცხვის სისტემები: RTO - 48 საათის განმავლობაში, RPO - მონაცემთა მინიმალური დაკარგვა (საათი თუ შესაძლებელია)

შენიშვნა: ზემოთ მოწოდებული RTOs და RPOs არის ზოგადი სახელმძღვანელო მითითებები და შეიძლება განსხვავდებოდეს ფილიალის სპეციფიკური საჭიროებებისა და მოთხოვნების მიხედვით. ფაქტობრივი ღირებულებები უნდა განისაზღვროს შესაბამის დაინტერესებულ მხარეებთან კონსულტაციისა და რისკის საფუძვლიანი შეფასების პროცესის მეშვეობით.

IT უწყვეტობის სტრატეგიები განსაზღვრავს სტრატეგიებს რისკების შესამცირებლად და IT სერვისის ხელმისაწვდომობის უზრუნველსაყოფად შეფერხებების დროს, მათ შორის: მონაცემთა სარეზერვო და აღდგენის პროცედურები, Reduntant სისტემები და failover მექანიზმები, Cloud-ზე დაფუძნებული გადაწყვეტილებები და დისტანციური წვდომის შესაძლებლობები, დაინტერესებული მხარეების საკომუნიკაციო არხები.

IT უწყვეტობის სტრატეგიები

მონაცემთა სარეზერვო და აღდგენის პროცედურები:

სტრატეგია: მონაცემთა სარეზერვო და აღდგენის ძლიერი პროცესი ხორციელდება, რათა უზრუნველყოს კრიტიკული მონაცემების ხელმისაწვდომობა და მთლიანობა მონაცემთა დაკარგვის ან სხვაგვარი დაზიანების შემთხვევაში.

ძირითადი მოქმედებები:

- სარეზერვო ასლის რეგულარულად შექმნა ყველა კრიტიკული მონაცემის ჩათვლით, მონაცემთა ბაზების, ფაილების და კონფიგურაციების ჩათვლით, კეთდება ყოველ ღამე ადგილობრივი მონაცემთა ცენტრიდან ვირტუალურ სერვერამდე.
- Webster ქსელის თითოეულ კომპიუტერს აქვს უნიკალური გამოსახულება ფიზიკური დაზიანების შემთხვევებისთვის.
- პერიოდული აღდგენის ტესტები ტარდება სარეზერვო პროცესის ეფექტურობის შესამოწმებლად.

Redundant სისტემები და Failover მექანიზმები:

სტრატეგია: განათავსეთ Redundant IT სისტემები და Failover მექანიზმები უწყვეტი სერვისის ხელმისაწვდომობის უზრუნველსაყოფად, მაშინაც კი, თუ პირველადი სისტემები განიცდიან ზიანს.

ძირითადი მოქმედებები:

- უნივერსიტეტი ახორციელებს Redundant Hardware კომპონენტებს (მაგ. სერვერები, გადამრთველები, კვების წყაროები) კრიტიკულ სისტემებში, რომელიმე ელემენტის გაუმართაობის შემთხვევაში განლაგებულია სარეზერვო რესურსები.
- ვინაიდან მონაცემთა ცენტრების უმეტესობა არის Cloud-ზე დაფუძნებული ფილიალმა დანერგა UPS, რომელიც დაკავშირებულია მთავარ სერვერთან, რაც

საკმაო დროის საშუალებას აძლევს ახალი მონაცემების სარეზერვო ასლის შექმნას და სისტემიდან სწორად გასვლას.

- ნებისმიერი შეფერხების შემთხვევაში, ფილიალის IT მენეჯერი დაუკავშირდება გლობალურ IT გუნდს, რათა გადახედონ ჩანაწერებს, რათა გამოავლინონ და შეამოწმონ პრობლემები იმ მიზნით, რომ სისტემა ფუნქციონირებდეს ისე, როგორც მოსალოდნელია.

Cloud-ზე დაფუძნებული გადაწყვეტილებები და დისტანციური წვდომის შესაძლებლობები:

სტრატეგია: ვებსტერის უნივერსიტეტი საქართველო იყენებს Cloud-ზე დაფუძნებულ გადაწყვეტილებებს და საშუალებას აძლევს დისტანციური წვდომის შესაძლებლობებს უწყვეტობის მხარდასაჭერად შეფერხებების დროს, რაც გავლენას ახდენს ფიზიკურ წვდომაზე კამპუსის ობიექტებზე.

ძირითადი მოქმედებები:

- ყველა კრიტიკული აპლიკაცია და მონაცემი მიგრირდება Cloud სერვისის რეპუტაციის მქონე პროვაიდერებში უსაფრთხოების ძლიერი ზომებით.
- Cloud-ზე დაფუძნებული სერვისები გვთავაზობენ მაღალ ხელმისაწვდომობას.
- სისტემებზე ყველა წვდომა ნებადართულია დისტანციურად, ყველა დაინტერესებული მხარის მიერ და კონტროლდება IT-ის მიერ მინიჭებული დონის მიხედვით.
- ყველა მომხმარებელი გადის ტრენინგს დისტანციური წვდომის პროცედურებისა და უსაფრთხოების საუკეთესო პრაქტიკის შესახებ.

ალტერნატიული საკომუნიკაციო არხები დაინტერესებული მხარეებისთვის:

სტრატეგია: ვებსტერის უნივერსიტეტს აქვს ალტერნატიული საკომუნიკაციო არხები, რათა ხელი შეუწყოს დაინტერესებულ მხარეებთან მუდმივ კომუნიკაციას შეფერხებების დროს.

ძირითადი მოქმედებები:

- ვებსტერი იყენებს მრავალ საკომუნიკაციო არხს, როგორიცაა ელფოსტა, ტექსტური შეტყობინებები პერსონალთან და სტუდენტებთან.
- საგანგებო სიტუაციების დროს ვებსტერის უნივერსიტეტი გასცემს Rave Alert-ს ყველა დაინტერესებულ მხარეს.

IT უწყვეტობის სტრატეგიის განხორციელებით, უნივერსიტეტმა მნიშვნელოვნად გაზარდა მდგრადობა პოტენციური შეფერხებების მიმართ და შეინარჩუნა აუცილებელი IT სერვისები რთულ სიტუაციებში. რეგულარული ტესტირება, ტრენინგი და კოორდინაცია დაინტერესებულ მხარეებთან აუცილებელი იყო ამ სტრატეგიების ეფექტურობის უზრუნველსაყოფად რეალურ სამყაროში შეფერხებების დროს. გარდა ამისა, სტრატეგიების პერიოდულად განახლებამ წარსული ინციდენტებიდან მიღებული გაკვეთილების საფუძველზე კიდევ უფრო გააუმჯობესა უნივერსიტეტის მზადყოფნა მომავალი მოვლენებისთვის.

შეიქმნა ინციდენტზე რეაგირების გეგმა, რომელშიც შედის ინციდენტზე რეაგირების ჯგუფი და განსაზღვრული როლები და პასუხისმგებლობები. დეტალურია IT ინციდენტების მოხსენებისა და უწყვეტობის გეგმის გააქტიურების პროცესი, ინციდენტების სიმძიმის შეფასებისა და საჭიროების შემთხვევაში ესკალაციის პროცედურები.

ინციდენტებზე რეაგირების გეგმა

ინციდენტებზე რეაგირების ჯგუფი და მათი როლები:

1. **ინციდენტებზე რეაგირების მენეჯერი:** საერთო პასუხისმგებლობა ინციდენტზე რეაგირების პროცესის მართვაზე, დაინტერესებულ მხარეებთან კოორდინაციასა და პრობლემის აღმოფხვრის ზედამხედველობაზე.

2. **ინფორმაციული ტექნოლოგიების მენეჯერი:** იძიებს და ამსუბუქებს უსაფრთხოებასთან დაკავშირებულ ინციდენტებს, როგორიცაა კიბერშეტევები, არაავტორიზებული წვდომა და მავნე პროგრამების ინფექციები.

3. **IT ოპერაციების გუნდი:** განიხილავს ინციდენტებს, რომლებიც დაკავშირებულია სისტემის და აპლიკაციის გაუმართაობასთან, აპარატურულ საკითხებთან და სერვისის შეფერხებებთან.

4. **კომუნიკაციების გუნდი:** მართავს შიდა და გარე კომუნიკაციას ინციდენტების დროს, რაც უზრუნველყოფს დაინტერესებული მხარეების ინფორმირებას სიტუაციისა და აღდგენის პროგრესის შესახებ.

5. **სამართლებრივი და შესაბამისობის ჯგუფი:** უზრუნველყოფს ინციდენტზე რეაგირების მოქმედებების შესაბამისობას სამართლებრივ, მარეგულირებელ და სახელშეკრულებო ვალდებულებებთან.

6. **ადამიანური რესურსების მენეჯერი:** ეხება ინციდენტებს, რომლებიც დაკავშირებულია ადამიანურ რესურსებთან, როგორიცაა შიდა საფრთხეები, პოლიტიკის დარღვევა ან პერსონალთან დაკავშირებული საკითხები.

IT ინციდენტების მოხსენება და უწყვეტობის გეგმის გააქტიურება:

IT ინციდენტების შეტყობინების პროცესი:

- არის გამოყოფილი ელექტრონული ფოსტა და ტელეფონის ნომერი დაუყოვნებლივი დახმარებისთვის;
- პერსონალი და სტუდენტები დაუყოვნებლივ აცნობებენ პრორექტორს ან IT მენეჯერს ნებისმიერი საეჭვო აქტივობის ან პოტენციური ინციდენტის შესახებ.
- რექტორის მოადგილე და IT მენეჯერი განსაზღვრავენ რა ინციდენტს წარმოადგენს IT ინციდენტი და შემდგომში ასრულებენ გეგმას.
- უწყვეტობის გეგმის გააქტიურება:
- ინციდენტზე რეაგირების მენეჯერი პასუხისმგებელია ინციდენტის სიმძიმის შეფასებაზე თავდაპირველი ანგარიშების საფუძველზე და განსაზღვროს, საჭიროა თუ არა უწყვეტობის გეგმის გააქტიურება.
- თუ ინციდენტი მნიშვნელოვან საფრთხეს უქმნის IT სერვისებსა და ოპერაციებს, ინციდენტზე რეაგირების მენეჯერი იწყებს უწყვეტობის გეგმის გააქტიურების პროცესს.

ინციდენტის სიმძიმისა და ესკალაციის შეფასების პროცედურები:

ინციდენტის სიმძიმის შეფასება:

- ინციდენტებზე რეაგირების ჯგუფი ატარებს ინციდენტის პირველად შეფასებას, რათა დადგინდეს მისი გავლენა და სიმძიმე კრიტიკულ IT სისტემებზე, მონაცემებსა და ოპერაციებზე.
- სიმძიმის დონეები შეიძლება დაიყოს კატეგორიებად (მაგ., დაბალი, საშუალო, მაღალი) წინასწარ განსაზღვრული კრიტერიუმების საფუძველზე, რომელიც ითვალისწინებს ფაქტორებს, როგორიცაა შეფერხების ხარისხი, მონაცემთა დაკარგვა და პოტენციური შედეგები.

ესკალაციის პროცედურები:

- სიმძიმის დონის მიხედვით, ინციდენტზე რეაგირების მენეჯერი აცნობს ინციდენტს შესაბამის დაინტერესებულ მხარეებს და უფრო მაღალ მენეჯმენტს ინფორმირებულობისა და გადაწყვეტილების მიღების მიზნით.
- ესკალაციის მატრიცა განსაზღვრავს ესკალაციის გზას სხვადასხვა სიმძიმის დონისთვის, რაც უზრუნველყოფს პერსონალის ინფორმირებას თითოეულ ეტაპზე.

სიმძიმის დონეებისა და ესკალაციის საფეხურების მაგალითები:

1. დაბალი სიმძიმის:

- ინციდენტებზე რეაგირების მენეჯერი აცნობებს შესაბამის გუნდს გამოძიებისა და გადაწყვეტისთვის.

- რეგულარულად განახლებული ინფორმაცია მიეწოდება დაინტერესებულ მხარეებს.

2. საშუალო სიმძიმის:

- ინციდენტებზე რეაგირების მენეჯერი ატყობინებს ადმინისტრაციის უფროსს რესურსების გაზრდისა და კოორდინაციისთვის.
- ინიცირებულია საკომუნიკაციო გეგმა ინციდენტის შესახებ დაზარალებული მხარეების ინფორმირებისთვის.

3. მაღალი სიმძიმე:

- ინციდენტებზე რეაგირების მენეჯერი აცნობებს ფილიალის მართვის ორგანოებს, მათ შორის რექტორს და რექტორის მოადგილეს.
- იწვევენ საგანგებო სიტუაციებზე რეაგირების შეხვედრას დამატებითი რესურსების მობილიზებისა და სწრაფი გადაწყვეტის მხარდაჭერის მიზნით.
- კომუნიკაციები გაფართოვდა, რათა მოიცავდეს უნივერსიტეტის საზოგადოებასთან ურთიერთობისა და იურიდიული გუნდები.

4. კრიტიკული სიმძიმე:

- მძიმე ინციდენტის შემთხვევაში შეიძლება შეიქმნას კრიზისების მართვის ფორმალური ჯგუფი, რომელშიც შედის სხვადასხვა უნივერსიტეტის წარმომადგენლები და გარე ექსპერტები.
- გააქტიურებულია კრიზისული კომუნიკაციის გეგმა დაინტერესებულ მხარეებთან, მედიასთან და საზოგადოებასთან კომუნიკაციის სამართავად.

ფილიალმა ჩამოაყალიბა და გააერთიანა ინციდენტებზე რეაგირების ეფექტური პროცედურები, რომლებიც ქმნიან ოპერატიული ჩარჩოს ქვაკუთხედს. ეს პროცედურები საშუალებას აძლევს ფილიალს სწრაფად აღმოაჩინოს, უპასუხოს და დაძლიოს IT ინციდენტები, ეფექტურად შეამსუბუქოს ნებისმიერი შეფერხება ჩვენს ოპერაციებში და შეინარჩუნოს პროცესების უწყვეტობა.

ასეთი მიდგომისთვის მთავარია ინციდენტზე რეაგირების გეგმის რეგულარული ტესტირება და მუდმივი დახვეწა, პრაქტიკა, რომელიც მიღებულია რეალურ სამყაროში არსებული ინციდენტებისაგან. ეს მუდმივი გაუმჯობესება უზრუნველყოფს, რომ ფილიალი იყოს კარგად მომზადებული და შეძლოს რეაგირების სტრატეგიების ადაპტირება მუდმივ გამოწვევებთან. ამ გეგმის დაცვით, ფილიალი აჩვენებს თავის ერთგულებას ინციდენტებზე რეაგირების ძლიერი და პროაქტიული შესაძლებლობების შესანარჩუნებლად.

აღდგენის პროცედურები:

- აღდგენის დეტალური პროცედურები: შექმნილია აღდგენის ყოვლისმომცველი პროცედურები თითოეული კრიტიკული IT სისტემისა და აპლიკაციისთვის. ეს პროცედურები ზედმიწევნით ასახავს ნაბიჯების ზუსტ თანმიმდევრობას, რომელიც უნდა შესრულდეს აღდგენის პროცესში.
- დაკისრებული პასუხისმგებლობები: გუნდის კონკრეტულ წევრებს დაეკისრათ პასუხისმგებლობები თითოეული აღდგენის ამოცანისთვის, რაც ხელს უწყობს აღდგენის გამარტივებულ და ორგანიზებულ ძალისხმევას.
- თანმიმდევრული აღდგენა: აღდგენის პროცესი მკაფიოდ იყო თანმიმდევრული, რაც იძლევა კრიტიკული IT სისტემებისა და აპლიკაციების სისტემატური და ეფექტური აღდგენის საშუალებას.
- ვერიფიკაციის საკონტროლო პუნქტები: საკონტროლო პუნქტები ინტეგრირებულია აღდგენის პროცესში, რათა უზრუნველყოფილი იყოს წარმატებული აღდგენის ვალიდაცია სხვადასხვა ეტაპზე, რაც უზრუნველყოფს აღდგენის სიზუსტეს.

1. კომუნიკაციის გეგმა: ფილიალმა ჩამოაყალიბა ძლიერი საკომუნიკაციო გეგმა, რათა უზრუნველყოს დაინტერესებული მხარეების კარგად ინფორმირებულობა IT შეფერხებების დროს:

- სპიკერები: გამოვლინდა ოფიციალური სპიკერ(ებ)ი და დაევალათ უშუალო კომუნიკაცია დაინტერესებულ მხარეებთან ინციდენტების დროს.
- მორგებული საკომუნიკაციო არხები: განისაზღვრა შესაბამისი საკომუნიკაციო არხები სხვადასხვა ტიპის ინციდენტისთვის, რაც უზრუნველყოფს ეფექტურ და მიზანმიმართულ კომუნიკაციას.

2. ტრენინგი და ტესტირება: ფილიალმა განახორციელა ტრენინგისა და ტესტირების ყოვლისმომცველი ინიციატივები:

- თანამშრომლების მომზადების პროგრამები: რეგულარული ტრენინგები ტარდება ინციდენტების დროს თანამშრომლების როლების გაცნობის მიზნით. თანამშრომლები იღებენ მითითებებს ინციდენტების მოხსენების, პროცედურების და კომუნიკაციის არხების ეფექტურად გამოყენების შესახებ.
- გეგმის რეგულარულად ტესტირება: იმიტირებული წვრთნები პერიოდულად იგეგმება სხვადასხვა IT ინციდენტების სიმულაციისთვის. ეს სავარჯიშოები აფასებენ ინციდენტზე რეაგირების პროცედურების ეფექტურობას.
- დაინტერესებული მხარეების მონაწილეობა: დაინტერესებული მხარეები სხვადასხვა სტრუქტურულ ერთეულებიდან აქტიურად არიან ჩართულნი ტესტირების პროცესში, რათა უზრუნველყონ ერთიანი და კოორდინირებული პასუხი.
- უწყვეტი გაუმჯობესება: იმიტირებული სავარჯიშოების შედეგები გაანალიზებულია გაუმჯობესების სფეროების დასადგენად. რეალური ინციდენტების გამოცდილება ინტეგრირებულია გეგმაში, რათა მუდმივად გაუმჯობესდეს მისი ეფექტურობა.

3. რესურსები: რესურსების მართვა არის უნივერსიტეტის IT უწყვეტობის გეგმის პრიორიტეტული ასპექტი:

- IT რესურსების ინვენტარიზაცია: უნივერსიტეტმა მოახდინა გეგმის განხორციელებისა და შენარჩუნებისთვის საჭირო აპარატურის, პროგრამული უზრუნველყოფის და ქსელის რესურსების კატალოგირება.
- ადამიანური რესურსების დაგეგმვა: განისაზღვრა ადამიანური რესურსების მოთხოვნები, მათ შორის უნარების ნაკრები და ტრენინგის საჭიროებები.
- ბიუჯეტის განაწილება: შემუშავებულია გამოყოფილი ბიუჯეტი IT უწყვეტობის გეგმის განხორციელებისა და შენარჩუნების მხარდასაჭერად.
- დაფინანსების წყაროები: დაფინანსების წყაროები, მათ შორის IT მენეჯერის ბიუჯეტი და ფილიალის საგანგებო სახსრები, გამოვლენილია უწყვეტი ძალისხმევის შესანარჩუნებლად.

4. გეგმის შენარჩუნება და განხილვა: გეგმის შენარჩუნება არის მუდმივი მცდელობა:

- რეგულარული მიმოხილვები: ფილიალი იცავს გეგმის რეგულარული განხილვის გრაფიკს, რათა უზრუნველყოს მისი შესაბამისობა.
- დოკუმენტირებული ცვლილებები: IT გარემოში ცვლილებები საგულდაგულოდ არის დოკუმენტირებული სიზუსტის შესანარჩუნებლად.
- ხარვეზების ანალიზი და გაძლიერება: პერიოდული ხარვეზების ანალიზი ტარდება გეგმის ხარვეზების გამოსავლენად. მიიღება მაკორექტირებელი მოქმედებები მისი ეფექტურობის გასაუმჯობესებლად.

ფილიალის მიერ IT უწყვეტობის გეგმის სისტემატური ორგანიზება ამ სექციებში ხაზს უსვამს მის ერთგულებას ეფექტური აღმოფხვრის შეფერხებების, კრიტიკული IT სერვისების დაცვას და ოპერაციული უწყვეტობის შენარჩუნებას. რეგულარული მიმოხილვების, ტესტირებისა და განახლებების ინტეგრაცია უზრუნველყოფს გეგმის მდგრად ეფექტურობას და ადაპტირებას დროთა განმავლობაში.