accountabilitylab PAKISTAN

پالیسی رپورٹ

ڈیجیٹائزیشن اور عوامی خدمات کی فراہمی

کیا جاننا اور کیا کرنا ضروری ہے؟

/accountlabpk pakistan.accountabilitylab.org

فہرست

جامع خُلاصہ 3
قابل اطلاق قوانین 4
پریونشن آف الیکٹرانک کرائمز ایکٹ 2016 4
معلومات تک رسائی کے حق کا قانون 2017 5
پرسنل ڈیٹا پروٹیکشن بل 6
ڈیجیٹل آلات، ڈیجیٹل پلیٹ فارمز کا استعمال اور بینڈ اوور پالیسی 7
عوامی خدمات کی فراہمی 8
سفارشات 8
مستحکم اور معیاری انٹرنیٹ کنکشن 8
مواصلاتی پلیٹ فارمز تک رسائی 9
غیر منظم پالیسی سازی 9
متحرک قانونی ماحول 9
ڈیجیٹل پالیسیوں کا جائزہ لینا 9
عوامی خدمات کے عمل کو جدید خطوط پر استوار کرنا 10

پالیسی رپورٹ

جامع خُلاصہ

آج کی باہم مربوط دنیا میں، ہر شعبے میں ڈیجیٹل ٹولز کا انضمام اور استعمال انتہائی ضروری ہے۔ اس پالیسی بریف میں متعلقہ قوانین، ڈیجیٹل ٹولز کے استعمال کے بہترین طریقہ کار اور ان پالیسیوں کو واضح کیا گیا ہے جنہیں موثر طریقے سے اختیار کرنا مختلف اداروں کے لیے ضروری ہے۔ اس کے علاوہ، اس مضمون میں ڈیجیٹائزیشن کے ذریعے شفافیت، قوانین یا اداروں تک رسائی اور عوامی خدمات کی فراہمی کو بہتر بنانے کے پہلوؤں کا جائزہ لیا گیا ہے اور ان چیلنجز پر قابو پانے کی سفارشات پیش کی گئی ہیں جو ترقی کی راہ میں رکاوٹ بن سکتے ہیں۔

پالیسی بریف کے پہلے حصے میں ڈیجیٹائزیشن سے متعلق قانونی فریم ورک پر روشنی ڈالی گئی ہے، جس میں "پریونشن آف الیکٹرانک کرائمز ایکٹ 2016" اور "رائٹ ٹو انفارمیشن ایکٹ 2017" شامل ہیں، مزید برآں اس میں "پرسنل ڈیٹا پروٹیکشن بل 2023" پر بھی بات کی گئی ہے۔ اس حصے میں ان قوانین کے تحت فرائض اور ذمہ داریوں کی وضاحت کی گئی ہے، جس سے ڈیجیٹل آلات اور پلیٹ فارمز کے مناسب استعمال کے بارے میں واضح رہنمائی ملتی ہے تاکہ قانونی مطابقت کو یقینی بنایا جا سکے اور ممکنہ قانونی پیچیدگیوں سے بچا جا سکے۔

پالیسی بریف کا دوسرا حصہ اداروں میں ڈیجیٹل پلیٹ فارمز کے استعمال اور ڈیجیٹل ذمہ داریوں کی حوالگی پر تفصیلی رہنمائی فراہم کرتا ہے۔ اس میں یہ ضروری ہدایات شامل ہیں کہ کون کون سے افراد کو مختلف ڈیجیٹل ٹولز تک رسائی حاصل ہونی چاہیے اور کون کون سے افراد کو ادارے کے آلات اور اکاؤنٹس کے استعمال کا اختیار ہونا چاہیے۔ اس حصے میں محفوظ اور مؤثر ڈیجیٹل طریقوں کو یقینی بنانے کے لیے احتیاطی تدابیر اور ہدایات کی جامع فہرست پیش کی گئی ہے، جس سے اداروں کے ڈیجیٹل ٹولز یا سوشل میڈیا پلیٹ فارمز تک غیر مجاز رسائی یا ان کے غلط استعمال کے خطرے کو کم کیا جا سکتا ہے۔

پالیسی بریف کا تیسرا حصہ ڈیجیٹائزیشن کے ذریعے عوامی خدمات کی فراہمی میں بہتری کے امکانات کا جائزہ لیتا ہے۔ یہ ڈیجیٹل ٹولز کے ذریعے عوامی خدمات کی کارکردگی، شفافیت اور رسائی میں بہتری کے پہلوؤں پر روشنی ڈالتا ہے، جس سے عوام اور خدمات فراہم کرنے والوں کے درمیان اعتماد اور شمولیت کو فروغ ملتا ہے۔

مضمون کے آخری حصے میں ان مختلف رکاوٹوں جیسے کہ تکنیکی، مالی اور انسانی وسائل کی کمی، کی نشاندہی کی گئی ہے جو ڈیجیٹائزیشن کے عمل کو متاثر کر سکتی ہیں۔ یہ حصہ ان چیلنجز سے نمٹنے کے لیے عملی سفارشات فراہم کرتا ہے، جس میں ہدفی سرمایہ کاری، صلاحیت سازی اور مضبوط ڈیجیٹل انفراسٹرکچر کی تعمیر کی سفارشات شامل ہیں۔ یہ اقدامات ڈیجیٹائزیشن کے لیے سازگار ماحول پیدا کرنے اور عوامی خدمات کی فراہمی میں ترقی اور جدت کو آگے بڑھانے کا ذریعہ ہیں۔

قابل اطلاق قوانین

پریوینشن آف الیکٹرانک کرائمز ایکٹ 2016

الیکٹرانک جرائم کی روک تھام کا قانون پیکا۔2016، جسے عموماً پاکستان کا سائبر کرائم قانون کہا جاتا ہے، آن لائن سرگرمیوں پر لاگو ہونے والا بنیادی قانونی فریم ورک ہے۔ یہ ایک فوجداری قانون ہے اور اس میں مختلف جرائم کی وضاحت کی گئی ہے۔ ذیلی جدول میں اس قانون کی دفعات 3 تا 26 میں ان جرائم کی تفصیل بیان کی گئی ہے۔

جُرم	سزا
3-معلوماتی نظام یا ڈیٹا تک غیر مجاز رسائی	تین ماہ تک قید یا پچاس ہزار روپے تک جرمانہ یا دونوں
4-ڈیٹا کی غیر مجاز نقل یا منتقلی	چھ ماہ تک قید یا ایک لاکھ روپے تک جرمانہ یا دونوں
5-معلوماتی نظام یا ڈیٹا میں مداخلت	دو سال تک قید یا پانچ لاکھ روپے تک جرمانہ یا دونوں
6۔اہم نوعیت کے انفراسٹرکچر کی غیر مجاز نقل یا منتقلی	تین سال تک قید یا دس لاکھ روپے تک جرمانہ یا دونوں
7۔اہم نوعیت کے انفراسٹرکچر کی غیر مجاز نقل یا منتقلی	پانچ سال تک قید یا پچاس لاکھ روپے تک جرمانہ یا دونوں
8۔اہم نوعیت کے انفراسٹرکچر کے ساتھ چھیڑ چھاڑ	سات سال تک قید یا ایک کروڑ روپے تک جرمانہ یا دونوں
9۔کسی جرم کی تشہیر	سات سال تک قید یا دس لاکھ روپے تک جرمانہ یا دونوں
10۔سائبر نظام کے ذریعے دہشت گردی	چودہ سال تک قید یا 5 کروڑ روپے تک جرمانہ یا دونوں
11۔نفرت انگیز مواد کی تشہیر	سات سال تک قید یا جرمانہ یا دونوں
12۔دہشت گردی کے مقصد کے تحت افراد کی بھرتی، مالی معاونت اور منصوبہ بندی	سات سال تک قید یا جرمانہ یا دونوں
13۔الیکٹرانک جعلسازی	تین سال تک قید یا ڈھائی لاکھ روپے تک جرمانہ یا دونوں
14۔الیکٹرانک پلیٹ فارم کے استعمال سے دھوکہ دہی	دو سال تک قید یا ایک کروڑ روپے تک جرمانہ یا دونوں
15۔جرم کے لیے آلات کی تیاری، حصول یا فراہمی	چھ ماہ تک قید یا پچاس ہزار روپے تک جرمانہ یا دونوں
16۔شناختی معلومات کا غیر مجاز استعمال	تین سال تک قید یا پچاس لاکھ روپے تک جرمانہ یا دونوں
17۔سم کارڈ وغیرہ کا غیر مجاز اجراء	تین سال تک قید یا پانچ لاکھ روپے تک جرمانہ یا دونوں
18۔سرکاری مواصلاتی آلات کے ساتھ چھیڑ چھاڑ یا تبدیلی	تین سال تک قید یا دس لاکھ روپے تک جرمانہ یا دونوں
19۔غیر مجاز معلومات کا حصول	دو سال تک قید یا پانچ لاکھ روپے تک جرمانہ یا دونوں
20۔کسی عام فرد کے خلاف جرم	تین سال تک قید یا دس لاکھ روپے تک جرمانہ یا دونوں
21۔کسی عام شخص کی عصمت کے خلاف جرم	پانچ سال تک قید یا پانچ لاکھ روپے تک جرمانہ یا دونوں سات سال تک کی معمولی قید اور پچاس لاکھ روپے جرمانہ دس سال تک کی معمولی قید اور جرمانے کے حوالے سے سابقہ سزاؤں کے لیے
22۔بچوں کی فحش تصاویر یا ویڈیوز بنانا	سات سال تک قید اور پانچ لاکھ روپے تک جرمانہ یا دونوں
22اے۔آن لائن گمراہ کرنا، ورغلانا اور سائبر پلیٹ فارم پر ترغیب	کم از کم 5 اور زیادہ سے زیادہ 10 سال تک قید اور کم از کم پانچ لاکھ اور زیادہ سے زیادہ دس لاکھ روپے تک جرمانہ
22بی۔تجارتی مقاصد کے لیے بچوں کا جنسی استحصال	کم از کم چودہ سال زیادہ سے زیادہ بیس سال تک قید اور کم از کم دس لاکھ روپے جرمانہ

جُرم	سزا
24۔آن لائن پلیٹ فارمز پر کسی کو ہراساں کرنا	پانچ سال تک قید یا ایک کروڑ روپے تک جرمانہ یا دونوں
24اے۔آن لائن پلیٹ فارم پر دھمکی دینا	کم از کم ایک سال اور زیادہ سے زیادہ 5 سال کی قید اور کم از کم ایک لاکھ اور زیادہ سے زیادہ 5 لاکھ روپے تک جرمانہ
25۔آن لائن پلیٹ فارمز پر غیر متعلقہ پیغامات بھیجنا	3 ماہ تک قید یا 50 ہزار سے 50 لاکھ روپے تک جرمانہ یا دونوں
26۔آن لائن پلیٹ فارم پر دھوکہ دہی/جعلسازی	3 سال تک قید یا 5 لاکھ روپے تک جرمانہ یا دونوں

وفاقی تحقیقاتی ایجنسی (ایف آئی اے) کو پیکا۔16 کے سیکشن 29 کے تحت تحقیقاتی ادارہ نامزد کیا گیا تاکہ اس قانون کے تحت جرائم کی تحقیقات اور مقدمات کی پیروی کی جاسکے۔2023 میں متعارف کرائی گئی ترامیم کے ذریعے پولیس کو بھی ایف آئی اے کے ساتھ ساتھ اس قانون کے تحت جرائم کا نوٹس لینے کے اختیارات دیے گئے۔2024 میں ایک نوٹیفکیشن جاری کیا گیا جس کے تحت نیشنل کرائم انویسٹیگیشن ایجنسی (NCCIA) کو ایف آئی اے کی جگہ تحقیقاتی ایجنسی نامزد کیا گیا اور اسے پیکا۔16 کے سیکشن 29 کے تحت جرائم کی تحقیقات اور مقدمات کی پیروی کرنے کی ذمہ داری دی گئی۔تاہم، اسی نوٹیفکیشن میں ایف آئی اے کو ایک سال تک اپنے فرائض انجام دینے کی اجازت دی گئی جب تک کہ این سی سی آئی اے مکمل طور پر فعال نہ ہو جائے۔ابھی تک اس سلسلے میں کوئی نوٹیفکیشن جاری نہیں ہوا، اور ایف آئی اے اپنے فرائض حسب معمول سرانجام دے رہا ہے۔حال ہی میں سامنے آنے والی خبروں کے مطابق، نیشنل فارنزک اور سائبر کرائم ایجنسی بھی قائم کی جا رہی ہے۔

اس وقت ایف آئی اے کے تحت مختلف شہروں میں پندرہ سائبر کرائم رپورٹنگ مراکز موجود ہیں۔شکایت درج کروانے کے لیے متاثرہ شخص کو تحریری شکایت جمع کرانی ہوتی ہے اور اس کے ساتھ لنکس، اسکرین شاٹس وغیرہ فراہم کرنے ہوتے ہیں۔ایک بار شکایت درج اور تصدیق ہو جانے کے بعد، شکایت کنندہ کو اپنا بیان ریکارڈ کروانا ہوتا ہے اور عدالت میں پیش ہونا پڑتا ہے۔پیکا۔16 کے تحت تین وجوہات پر ایف آئی اے براہ راست ایف آئی آر درج کر سکتا ہے اور تحقیقات کر سکتا ہے۔تاہم، دیگر جرائم کے لیے انہیں پہلے پیکا۔16 کی خصوصی عدالت سے مجسٹریٹ کی اجازت حاصل کرنا ہوتی ہے اور پھر آگے بڑھنا ہوتا ہے۔الیکٹرانک جرائم کی تفتیش کے قواعد 2018 میں اس طریقہ کار کو مزید تفصیل سے بیان کیا گیا ہے۔

اس ایکٹ کے تحت ڈیٹا کی سرچ و ضبطی، ڈیٹا کو افشاء کرنے اور کسی مشتبہ سرگرمی کی نگرانی کے لیے وارنٹ یا عدالت کی اجازت درکار ہوتی ہے، لیکن عملی طور پر وارنٹ حاصل نہیں کیے جاتے۔اس کے بجائے، قانون کی ایسی شقوں کا استعمال کرتے ہوئے ایف آئی آر درج کی جاتی ہے، گرفتاری کی جاتی ہے اور آلات اور ڈیٹا تک رسائی حاصل کی جاتی ہے جن کے تحت ایف آئی اے کو براہ راست کاروائی کا اختیار حاصل ہے۔قانون تقاضا کرتا ہے کہ ضبطی کے وقت ثبوتوں کو پورا کیا جائے اور جس شخص کا آلہ ضبط کیا جا رہا ہو، اس سے ضبطی میمو پر دستخط لیے جائیں۔یہ ثبوت کے طور پر مقدمے کے دوران شامل کیا جاتا ہے۔

مواد کو بلاک کرنے اور ہٹانے کے لیے پاکستان ٹیلی کمیونیکیشن اتھارٹی کو پیکا۔16 کے سیکشن 37 کے تحت اختیار دیا گیا ہے۔کچھ درخواستوں کی نوعیت جو پی ٹی اے نے پلیٹ فارمز کو بھیجی ہیں، ان کے شفافیت کی رپورٹس میں درج ہیں۔آن لائن پلیٹ فارمز پر متعدد پابندیاں، جیسے کہ پلیٹ فارمز پر مکمل پابندی، مختلف ہائی کورٹس میں زیر سماعت رہ چکی ہیں۔مقامی قوانین کے علاوہ متبادل طور پر، سوشل میڈیا پلیٹ فارمز پر مواد کو براہ راست ان کی کمیونٹی گائیڈ لائنز یا قواعد کے تحت رپورٹ کیا جاسکتا ہے، جس کے نتیجے میں پوسٹس، اکاؤنٹس کی معطلی یا اکاؤنٹس پر مخصوص پابندیاں عائد کی جاسکتی ہیں۔

معلومات تک رسائی کے حق کا قانون 2017

آئین کے آرٹیکل 19اے کے تحت وفاقی اور صوبائی سطح پر معلومات تک رسائی کے قوانین بنائے گئے ہیں تاکہ شہریوں کو سرکاری اداروں سے معلومات حاصل کرنے کا حق دیا جاسکے۔یہ قوانین درخواستوں پر عمل کرنے کے لیے مخصوص وقت کے فریمز کا تعین کرتے ہیں، سرکاری اداروں کو جواب دہ بناتے ہیں اور اگر کسی عوامی ادارے نے درخواست کا جواب نہیں دیا تو شکایت کے ازالے کے عمل کی وضاحت کرتے ہیں۔

وفاقی سطح پر معلومات تک رسائی کا قانون 2017 نافذ العمل ہے۔اس قانون کے تحت سرکاری اداروں پر معلومات کی افشاء کے حوالے سے کچھ ذمہ داریاں عائد کی گئی ہیں۔مثلاً:

- کیا ادارہ معلومات تک رسائی کے قانون 2017 کے سیکشن 5 کے تحت ایک وفاقی عوامی ادارے کے طور پر اپنی ذمہ داریوں کی تعمیل کر رہا ہے؟ (متعلقہ سیکشن کی تفصیلات نیچے دی گئی ہیں)

5۔ ریکارڈ کی اشاعت اور دستیابی

(1)۔ ہر سرکاری ادارے کا پرنسپل آفیسر اس ایکٹ کے آغاز کے چھ ماہ کے اندر اس بات کو یقینی بنائے گا کہ درج ذیل زمروں کی معلومات اور ریکارڈ مناسب طریقے سے، بشمول انٹرنیٹ پر اپ لوڈ کرنے کے، شائع کیے جائیں تاکہ یہ محدود وسائل کے ساتھ مناسب پابندیوں کے ساتھ قابل رسائی ہوں:

(الف)۔ سرکاری ادارے کی تنظیم اور افعال، فرائض، اختیارات اور عوام کو فراہم کی جانے والی کوئی بھی خدمات کی تفصیل، بشمول اس کے افسران اور ملازمین کی ڈائریکٹری جس میں ان کے فرائض اور کاموں کی نشاندہی کی گئی ہو اور ان کی متعلقہ تنخواہوں، مراعات اور فوائد کا ذکر ہو؛

(ب)۔ سرکاری ادارے پر لاگو قوانین، ان کے نفاذ کی تاریخ کے ساتھ، قواعد، ضوابط، بائی لاز، احکامات اور نوٹیفکیشن وغیرہ

ج)۔ سرکاری ادارے کی طرف سے بنائے گئے یا اپنائے گئے عمومی اطلاق کے مادی یا عملی ضوابط اور قواعد، بشمول کوئی بھی پالیسیاں جو اس کے ملازمین استعمال کرتے ہیں

(د)۔ اہم پالیسیوں اور فیصلوں سے متعلقہ حقائق اور پس منظر کی معلومات جو اپنائی گئی ہیں، کے ساتھ سرکاری ادارے کی طرف سے اپنائی گئی پالیسیوں کی تفصیلات

ایسے معیار یا رہنما اصول جن کی بنیاد پر سرکاری ادارہ اختیارات کا استعمال کرتا ہے؛

(الف)۔ وہ شرائط جن پر عوام کسی سرکاری ادارے سے لائسنس، اجازت نامہ، منظوری، گرانٹ، الاٹمنٹ یا کسی بھی نوعیت کے دیگر فوائد حاصل کر سکتے ہیں یا جن پر لین دین، معاہدے بشمول ملازمت کے معاہدے سرکاری ادارے کے ساتھ کیے جا سکتے ہیں، ساتھ ہی ان افراد کی تفصیلات جنہیں عوامی ادارے کی طرف سے کوئی رعایت، اجازت نامہ، لائسنس یا اختیار دیا گیا ہے

(ب)۔ فیصلے سازی کا عمل جیسا کہ وفاقی حکومت کے سیکرٹریٹ کے ہدایات نامہ۔ 2004 میں بیان کیا گیا ہے اور ایسی کوئی بھی ہدایات جو اس وقت نافذ العمل ہیں تاکہ عوام فیصلوں میں شمولیت کر سکیں یا ان کے بارے میں مشورہ کر سکیں

(ج) سرکاری ادارے کا تفصیلی بجٹ، بشمول تجویز کردہ اور اصل اخراجات، ابتدائی یا نظر ثانی شدہ محصولات کے اہداف، اصل آمدنی کی رسیدیں، منظور شدہ بجٹ میں نظر ثانیات اور اضافی بجٹ

(د) وہ ذرائع جن سے سرکاری ادارے کے کنٹرول میں موجود معلومات بشمول نام، عہدہ اور رابطے کی تفصیلات، حاصل کی جا سکتی ہیں اور مقرر کردہ فیس کی تفصیلات جو اس کے ساتھ درکار ہے

(ہ) رپورٹس بشمول کارکردگی رپورٹس، آڈٹ رپورٹس، تشخیصی رپورٹس، انکوائری یا تحقیقاتی رپورٹس اور دیگر رپورٹس جو حتمی شکل اختیار کر چکی ہوں

(و) وہ دیگر امور جو عوامی ادارے کے پرنسپل افسر کو عوامی مفاد میں شائع کرنے کے لیے موزوں لگیں؛

(ز) وہ دیگر معلومات جن کی وضاحت کی گئی ہے اور

(ط) عوامی مقامات پر کیمروں کی فوٹیجز، جہاں بھی دستیاب ہوں، جو کسی جرم سے متعلق ہوں

بشرطیکہ اگر معلومات یا ریکارڈ کا تعلق 2008 سے پہلے کے دور سے ہے تو اسے معقول وقت کے اندر شائع کیا جائے۔

- کیا سیکشن 5 کے تحت انکشاف کا کمپیوٹرائزڈ ریکارڈ دستیاب ہے؟
- کیا معلومات کی درخواستوں کو نمٹانے کے لیے کوئی نامزد افسر/پرنسپل انفارمیشن آفیسر موجود ہے؟

پرسنل ڈیٹا پروٹیکشن بل

پاکستان میں اس وقت ڈیٹا کے تحفظ کا کوئی قانون موجود نہیں ہے، تاہم ایک مسودہ قانون زیر بحث ہے جو منظوری کے بعد نافذ کیا جا سکتا ہے اور یہ شہریوں کے ڈیٹا کی دیکھ بھال کرنے والوں پر ذمہ داریاں عائد کرے گا۔ انفارمیشن ٹیکنالوجی سے وابستہ کئی کمپنیاں جو بین الاقوامی کلائنٹس کے ساتھ کام کرتی ہیں، عام طور پر جنرل ڈیٹا پروسیسنگ ریگولیشن (GDPR) کی ضروریات پر عمل کرتی ہیں تاکہ متعلقہ قوانین کی پیروی کی جا سکے۔ ڈیٹا کے تحفظ کے کسی بھی اچھے قانون کا مقصد فرد کو اپنے ڈیٹا پر خود مختاری فراہم کرنا اور اس کی رازداری کی حفاظت کو یقینی بنانا ہوتا ہے۔ اگر آپ کسی بھی شکل میں ڈیٹا جمع کر کے معلومات کو اپنے پاس محفوظ کرتے ہیں تو ذیل میں تجویز کردہ بہترین طریقوں کو خاص طور پر اپنانا ضروری ہے، کیونکہ ڈیٹا تحفظ کے قانون کے جلد لاگو ہونے کی توقع ہے۔ ان طریقوں کو درج ذیل سوالات کے ذریعے واضح کیا گیا ہے:

- آپ کون سا ڈیٹا جمع کرتے ہیں؟
- ڈیٹا کیسے جمع، محفوظ اور استعمال کیا جاتا ہے؟
- یہ ڈیٹا کس سے اور کس مقصد کے جمع کیا جاتا ہے؟
- آپ جس شخص سے ڈیٹا جمع کر رہے ہیں کیا وہ اس بات سے آگاہ ہے کہ اس کا ڈیٹا جمع کیا جا رہا ہے اور اس کا مقصد کیا ہے؟
- جس شخص کا ڈیٹا آپ جمع کر رہے ہیں، کیا اس نے اس کے جمع کرنے اور استعمال کرنے کی اجازت دی ہے؟
- ادارے کے اندر اس ڈیٹا تک کس کی رسائی ہے؟
- ڈیٹا کو کس طرح محفوظ اور خفیہ رکھا جا رہا ہے؟
- ڈیٹا کب تک کے لیے محفوظ کیا جائے گا؟
- کیا کوئی ڈیٹا کو تلف کرنے کی پالیسی موجود ہے؟
- اگر ڈیٹا میں کوئی خلاف ورزی ہوتی ہے تو کیا ہو گا؟

اگرچہ اس وقت کوئی قابل اطلاق ڈیٹا تحفظ کا قانون موجود نہیں ہے، لیکن ادارے کی سطح پر ڈیٹا جمع کرنے اور استعمال کے بارے میں آگاہی ضروری ہے تاکہ رازداری اور خفیہ معلومات کے حوالے سے بہترین طریقوں کو برقرار رکھا جا سکے۔ جب قانون نافذ ہو گا، تو قانونی ذمہ داریاں عائد ہوں گی جو تعمیل کا تقاضا کریں گی۔ پہلے سے بنیادی علم رکھنے سے ادارے کو سمجھ بوجھ اور بعد میں تعمیل میں مدد ملے گی۔

ڈیجیٹل آلات، ڈیجیٹل پلیٹ فارمز کا استعمال اور ہینڈ اوور پالیسی

کسی بھی ادارے کے لیے ڈیجیٹل آلات اور پلیٹ فارمز کے استعمال اور ہینڈ اوور کی پالیسی کا ہونا بہت ضروری ہے۔ یہ ملازمین کے لیے اس بات کو یقینی بناتا ہے کہ انہیں کام کے لیے دیے گئے آلات اور سوشل میڈیا یا پلیٹ فارمز کے استعمال کے دوران کون سے طریقے اپنانے چاہئیں۔ چاہے وہ فراہم کردہ آلات ہوں یا پلیٹ فارمز پر موجود گی، یہ سب ایک تحریری ہدایت نامے کے ذریعے بطور پالیسی درج ذیل امور کا احاطہ کرتی ہو:

- ای میل اور سوشل میڈیا اکاؤنٹس تک کس کو رسائی حاصل ہے؟
- کس کو اکاؤنٹس تک رسائی حاصل کرنے، پوسٹ کرنے اور سوالات یا کمنٹس جواب دینے کی اجازت ہے؟
- مواصلات یا پوسٹ شائع ہونے سے پہلے کون ان کی جانچ کرتا ہے؟
- پوسٹ کرنے یا جواب دینے کے لیے رہنما اصول کیا ہیں؟
- پالیسی کی خلاف ورزی کا کیا نتیجہ ہو گا؟

قانونی ڈھانچوں اور ذمہ داریوں کی وجہ سے یہ جاننا بھی ضروری ہے۔

- انٹرنیٹ کنکشن کس کے نام پر رجسٹرڈ ہے؟
- ڈیجیٹل آلہ (فون کے معاملے میں) کس کے نام پر رجسٹرڈ ہے؟

کسی قانون نافذ کرنے والے ادارے کی درخواست پر کوئی ردعمل سب سے پہلے انٹرنیٹ کنکشن (آئی پی ایڈریس کی بنیاد پر) اور پھر متعلقہ آلہ سے منسلک ہو گا، اور جس شخص کے نام یہ رجسٹرڈ ہو گا، اسے سب سے پہلے سوالات کا سامنا کرنا پڑے گا اور وہ ذمہ دار ہو گا۔ اگر کوئی ملازم جو ادارے کی جانب سے سوشل میڈیا اکاؤنٹس کو دیکھ رہا ہے، اس کا آلہ یا اکاؤنٹ (چوری یا خلاف ورزی کی وجہ سے) متاثر ہوتا ہے یا اگر کوئی ملازم جو سوشل میڈیا اکاؤنٹس کا ذمہ دار ہو ملازمت چھوڑ دیتا ہے، تو درج ذیل اقدامات کو یقینی بنائیں:

- ان کی ادارے کی ای میل اور ادارے کے سوشل میڈیا اکاؤنٹس تک رسائی ختم کر دی جائے۔
- اکاؤنٹس کے پاس ورڈز اور ان سے منسلک نمبرز تبدیل کیے جائیں۔
- ادارے میں موجود دیگر افراد کو اس بارے میں مطلع کیا جائے۔

اس کے علاوہ، بنیادی ڈیجیٹل شفافیت کے اقدامات اپنانے ضروری ہیں، جن میں درج ذیل امور شامل ہیں:

- سوشل میڈیا اکاؤنٹس کے لیے معمول سے ہٹ کر اور مضبوط پاس ورڈز ہونا چاہیے۔
- تمام اکاؤنٹس کے لیے دوہری تصدیق کو فعال کیا جائے۔
- ریکوری کے لیے بیک اپ معلومات دستیاب ہونی چاہئیں۔
- تمام آلات پر باقاعدگی سے اینٹی وائرس اسکین چلائے جائیں۔
- لنکس پر کلک کرتے وقت اور فائلیں ڈاؤن لوڈ کرتے وقت احتیاط برتی جائے۔

ڈیجیٹل آلات اور پلیٹ فارمز کے استعمال اور ہینڈ اوور پالیسی کو تحریری شکل میں رکھنے کے ساتھ ساتھ، ملازمین کے ساتھ سیشنز منعقد کرنا اور ان پالیسیوں کی کارکردگی کا جائزہ لینا بھی ضروری ہے۔ تکنیکی ڈھانچے کا انتظام کرنا اور بنیادی ڈیجیٹل شفافیت کو یقینی بنانا شاید آسان ہو، لیکن ایڈیٹوریل پہلو خاص طور پر سوشل میڈیا پلیٹ فارمز یا براہِ راست رابطے کے ذریعے عوامی روابط کرنے والوں کے لیے مشکل ہو سکتا ہے۔ ایڈیٹوریل فیصلے کسی خاص وقت میں کی جانے والی رائے پر مبنی ہوتے ہیں اور اگر یہ فیصلے غلط ہوں، تو ان کے منفی نتائج بھی ہو سکتے ہیں۔ اس لیے، تحریری ضابطہ کے ساتھ بات چیت اور مباحثہ کے ذریعے سمجھ بوجھ حاصل کرنا شفافیت کے لیے ایک اچھا عمل ہے۔

عوامی خدمات کی فراہمی

کسی ایسے ادارے کے لیے جو کسی بھی قسم کی عوامی خدمات فراہم کرتا ہو، عوامی نظر میں آنا بہت اہم ہے۔ لیکن نظر آنے کے ساتھ ساتھ اس تک عوامی رسائی بھی ضروری ہے۔

- لوگ آپ تک کیسے پہنچ سکتے ہیں؟
- وہ آپ کے کام کے بارے میں کیسے باخبر رہتے ہیں؟
- کیا آپ عوامی خدمات کے پیغامات جاری کرتے ہیں؟
- آپ عوامی سطح پر کس طرح بات چیت کرتے ہیں؟ کن ذرائع سے؟
- کیا آپ کے پاس کوئی براڈکاسٹ لسٹ موجود ہے؟

عموماً، کسی ادارے کی ویب سائٹ، سوشل میڈیا اکاؤنٹس اور ہیلپ لائن یا فون نمبر کے ذریعے عوامی رابطے کا کوئی طریقہ ہوتا ہے۔ ان ذرائع کو اپ ڈیٹ اور فعال رکھنا بھی ضروری ہوتا ہے۔ اگر ادارے کسٹمرز یا صارفین کے ساتھ لین دین کرتا ہے، تو ہیلپ لائنز یا ہیلپ ڈیسک کا قیام، جو خودکار نظام کے تحت شکایتی نمبر اور تازہ ترین معلومات فراہم کرتے ہیں، اچھی پریکٹس ہے۔ خودکاری کے علاوہ، انسانی رابطے کا عنصر اعتماد سازی میں مددگار ثابت ہوتا ہے۔ خواندگی کی سطح کو مدنظر رکھتے ہوئے، خودکاری کے باوجود سہولت کی فراہمی کی ضرورت برقرار رہے گی۔ کوئی بھی خودکار پیغامات کم از کم دو زبانوں، انگریزی اور اردو، میں ہونے چاہئیں۔

سوالناموں کے ذریعے عوام کی رائے لینا ادارے کے اندرونی امور کے لیے فائدہ مند ہوتا ہے۔ ادارہ چاہے سرکاری ہو یا نجی شعبے سے، اگر وہ عوام کے ساتھ لین دین کرتا ہے تو درج ذیل باتوں کو واضح طور پر بیان کیا جانا چاہیے:

- ادارے کا کردار اور مینڈیٹ
- کس سے اور کیسے رابطہ کریں
- کسی مسئلے کی صورت میں کیا کرنا چاہیے

ایسے دور میں جہاں غلط معلومات اور پروپیگنڈا عام ہو، اس کا تدارک کرنے کے بہترین طریقوں میں سے ایک یہ ہے کہ ادارہ اپنی ویب سائٹ اور سوشل میڈیا اکاؤنٹس کے ذریعے درست معلومات فراہم کرے اور غلط فہمیوں کا ازالہ کرے، پریس ریلیز یا اخباری بیان کے ذریعے بھی معلومات کو درست کیا جا سکتا ہے۔

سفارشات

ڈیجیٹلائزیشن کی صلاحیت کو مکمل طور پر استعمال کرنے کے لیے مستحکم اور معیاری انٹرنیٹ کنکشن کے ساتھ ساتھ ان پلیٹ فارمز تک مسلسل رسائی کو یقینی بنانا بہت ضروری ہے جو مواصلات، کاروبار، اور عوامی خدمات کی فراہمی کے لیے استعمال ہوتے ہیں۔ اس شعبے میں سب سے بڑی رکاوٹ غیر منظم پالیسی سازی ہے، جس کے تحت کبھی کبھی انٹرنیٹ سروسز کو مکمل طور پر معطل کر دیا جاتا ہے یا پلیٹ فارمز تک رسائی غیر معینہ مدت کے لیے محدود کر دی جاتی ہے۔ انٹرنیٹ کی رفتار کم ہونے سے عوامی شمولیت اور بین الاقوامی پلیٹ فارمز پر پاکستانیوں کی موجودگی متاثر ہوتی ہے، جس سے مواصلات، خدمات کی فراہمی، ملکی ساکھ، اور سرمایہ کاری پر منفی اثرات مرتب ہوتے ہیں۔

مستحکم اور معیاری انٹرنیٹ کنکشن:

- اہمیت: مستحکم انٹرنیٹ کنکشن مواصلات، کاروباری سرگرمیوں، تعلیم، اور عوامی خدمات کے لیے بنیادی اہمیت کا حامل ہے۔ مستحکم کنکشن معلومات، خدمات، اور عالمی نیٹ ورکس تک آسان رسائی کو یقینی بناتا ہے، جو ملک کی معاشی اور سماجی ترقی کے لیے ضروری ہے۔
- چیلنجز: بار بار انٹرنیٹ کی بندش، سست رفتار، اور علاقائی تفاوت مؤثر مواصلات میں رکاوٹ بنتے ہیں اور ڈیجیٹل پلیٹ فارمز میں شرکت کو محدود کرتے ہیں، جس سے کاروباری مواقع اور انفرادی ترقی متاثر ہو سکتی ہے۔

سفارشات

- انٹرنیٹ کے بنیادی ڈھانچے کو اپ گریڈ کرنے اور شہری اور دیہی علاقوں میں پھیلانے کے لیے سرمایہ کاری کی جائے۔
- انٹرنیٹ سروسز فراہم کرنے والوں کے درمیان مقابلے کو فروغ دینے والی پالیسیاں نافذ کی جائیں تاکہ خدمات کا معیار بہتر ہو۔
- ایسے ریگولیٹری فریم ورک قائم کیے جائیں جو بغیر کسی غیر ضروری رکاوٹوں کے مسلسل اور قابل اعتماد انٹرنیٹ خدمات کو یقینی بنائیں۔

مواصلاتی پلیٹ فارمز تک رسائی:

- اہمیت: سوشل میڈیا، ای میل سروسز، اور تعاون کے ٹولز جیسے پلیٹ فارمز مواصلات، برانڈنگ، اور عوام تک رسائی کے لیے اہم ہیں۔ یہ پلیٹ فارم کاروباری اداروں کو اپنی مصنوعات کی مارکیٹنگ، گاہکوں کے ساتھ رابطہ، اور برانڈ کی شناخت قائم کرنے میں مدد دیتے ہیں۔
- چیلنجز:۔ کچھ پلیٹ فارمز پر عارضی یا غیر معینہ پابندیاں مواصلات اور برانڈنگ کی کوششوں میں رکاوٹ ڈالتی ہیں، جس سے وسیع تر صارفین تک پہنچنا اور بین الاقوامی تعاون میں مشکلات پیدا ہوتی ہیں۔

سفارشات

- ڈیجیٹل پلیٹ فارمز کی ریگولیشن کے لیے واضح ہدایات تیار کی جائیں تاکہ غیر ضروری پابندیوں سے بچا جا سکے
- پابندیوں کو شفاف، جائز، اور کم سے کم اثر رکھنے والا بنایا جائے تاکہ مسلسل رسائی برقرار رہے۔
- ڈیجیٹل خواندگی کو فروغ دیا جائے تاکہ ان پلیٹ فارمز کا مؤثر استعمال ممکن ہو۔

غیر منظم پالیسی سازی:

- اہمیت: مستقل اور سوچ بچار پر مبنی پالیسیاں ایک مستحکم ڈیجیٹل ماحول کے فروغ کے لیے ضروری ہیں۔ غیر منظم یا ردعمل پر مبنی پالیسی سازی غیر یقینی صورتحال پیدا کرتی ہے، جو کاروباروں اور افراد کے لیے مشکلات پیدا کرتی ہے۔
- چیلنجز: پالیسیاں جو بار بار تبدیل کی جاتی ہیں یا بغیر مناسب مشاورت کے لاگو کی جاتی ہیں، غیر یقینی صورتحال کا سبب بنتی ہیں، جس سے کاروباروں اور افراد کے لیے منصوبہ بندی اور مؤثر آپریشن مشکل ہو جاتا ہے۔

سفارشات

- پالیسی سازی کے عمل میں عوامی اور نجی شعبے کے اسٹیک ہولڈرز کو شامل کرنے کے لیے باہمی تعاون پر مبنی فضا قائم کی جائے۔
- نئی پالیسیوں کے نفاذ سے پہلے ان کے ممکنہ اثرات کو سمجھنے کے لیے اثرات کی تشخیص کی جائے۔
- طویل مدتی حکمت عملی تیار کی جائے جو ڈیجیٹل ترقی اور ریگولیشن کے لیے واضح سمت فراہم کریں۔

متحرک قانونی ماحول:

- اہمیت: تازہ ترین قانونی فریم ورک سے باخبر رہنا تعمیل کو یقینی بنانے اور ڈیجیٹل مواقع سے فائدہ اٹھانے کے لیے ضروری ہے۔ واضح طور پر بیان کردہ اور مستقل طور پر نافذ کردہ قوانین اعتماد پیدا کرتے ہیں اور سرمایہ کاری کی حوصلہ افزائی کرتے ہیں۔
- چیلنجز: قوانین میں تیزی سے تبدیلیاں اور غیر مستقل نفاذ الجھن پیدا کر سکتے ہیں اور نئے ضوابط کے مطابق مؤثر طریقے سے ڈھلنے میں رکاوٹ بنتے ہیں۔

سفارشات

- قانونی تبدیلیوں اور ان کے عملی اثرات کی وضاحت کرنے والے آسان رسائی والے ٹولز تیار کیے جائیں۔
- کاروباری اور سرکاری اداروں کے لیے نئے ضوابط پر باقاعدہ تربیت اور اپ ڈیٹس فراہم کی جائیں۔
- ڈیجیٹل قوانین کے نفاذ میں شفافیت اور مستقل مزاجی کو فروغ دیا جائے۔

ڈیجیٹل پالیسیوں کا جائزہ لینا:

- اہمیت: ڈیجیٹل پالیسیوں کو باقاعدگی سے اپ ڈیٹ کرنا یہ یقینی بناتا ہے کہ وہ نئی ٹیکنالوجیز، عملی طریقوں اور ورک فورس کی کارکردگی کا مؤثر جواب دیں۔ اس موافقت سے کارکردگی اور تعمیل برقرار رکھنے میں مدد ملتی ہے۔
- چیلنجز: پرانی پالیسیوں کا غیر مؤثر یا نقصان دہ ہونا ممکن ہے، جس سے کارکردگی میں رکاوٹیں اور ممکنہ قانونی مسائل پیدا ہو سکتے ہیں۔

سفارشات

- ڈیجیٹل پالیسیوں کے جائزے کے لیے ایک سائیکل قائم کیا جائے تاکہ ان کا وقتاً فوقتاً جائزہ لیا جا سکے اور انہیں اپ ڈیٹ کیا جا سکے۔
- پالیسی کی نظر ثانی کے عمل میں مختلف ٹیموں کو شامل کیا جائے تاکہ مختلف نقطہ نظر اور ضروریات کو سمجھا جا سکے۔
- ٹیکنالوجی کے رجحانات اور قانونی تبدیلیوں پر نظر رکھیں تاکہ پالیسیوں کو پیشگی طور پر اپ ڈیٹ کیا جا سکے۔

عوامی خدمات کے عمل کو جدید خطوط پر استوار کرنا:

- اہمیت: جدید ڈیجیٹل ٹولز اور مواصلاتی طریقوں کا استعمال عوامی خدمات کی کارکردگی، رسائی اور شفافیت کو بہتر بناتا ہے۔ یہ عوامی خدمات کے ساتھ شہریوں کی شمولیت اور اطمینان کو بڑھا سکتا ہے۔
- چیلنجز: تبدیلی کے خلاف مزاحمت، ڈیجیٹل انفراسٹرکچر کی کمی، اور محدود ڈیجیٹل خواندگی عوامی خدمات کو جدید رُخ دینے میں رکاوٹ بن سکتے ہیں۔

سفارشات:

- جدید عوامی خدمات کے پلیٹ فارمز کے نفاذ کے لیے ڈیجیٹل انفراسٹرکچر میں سرمایہ کاری کریں۔
- عوامی خدمات پر مامور ملازمین کے لیے ان کی ڈیجیٹل مہارتوں کو بہتر بنانے کے لیے تربیتی پروگرام کرواتے رہیں۔
- ای گورنمنٹ خدمات کو اپنانے کی حوصلہ افزائی کریں اور شہریوں کو ان خدمات کے مؤثر استعمال کے لیے مدد فراہم کریں۔
- عوامی خدمات اور فیصلہ سازی کے عمل کو بہتر بنانے کے لیے ڈیٹا تجزیات کا استعمال کریں۔

پالیسی رپورٹ